(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 November 2002 (14.11.2002)

PCT

(10) International Publication Number
WO 02/091316 A1

(51) International Patent Classification[7]: G07F 7/10, H04L 29/06

(21) International Application Number: PCT/EP02/03930

(22) International Filing Date: 9 April 2002 (09.04.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

09/844,246	30 April 2001 (30.04.2001)	US
09/844,439	30 April 2001 (30.04.2001)	US
09/844,272	30 April 2001 (30.04.2001)	US

(71) Applicant *(for all designated States except US)*: **ACTIVCARD** [FR/FR]; 24-28, avenue du Général de Gaulle, F-92156 Suresnes Cedex (FR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **AUDEBERT, Yves, Louis, Gabriel** [FR/US]; 237 Forrester Road, Los Gatos, CA 95032 (US). **CLEMOT, Olivier** [FR/FR]; 23, rue Jules Parent, F-92500 Rueil-Malmaison (FR).

(74) Agent: **CABINET JP COLAS**; 37, avenue Franklin D. Roosevelt, F-75008 Paris (FR).

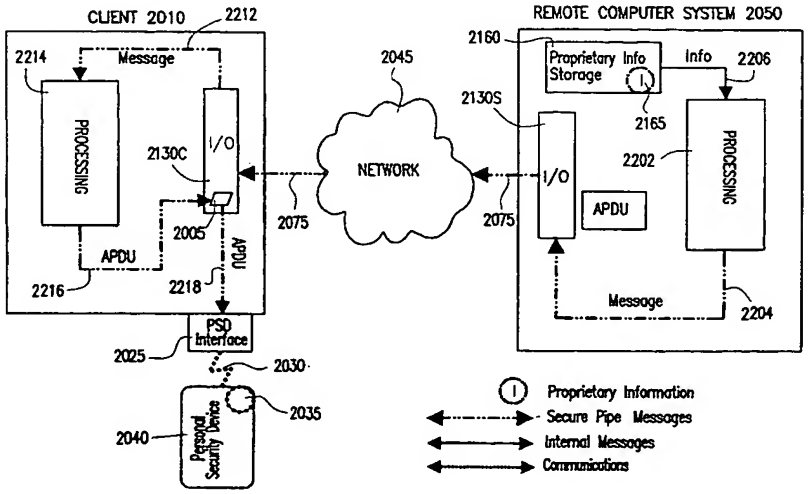
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR REMOTE ACTIVATION AND MANAGEMENT OF PERSONAL SECURITY DEVICES



(57) Abstract: The present invention provides a method for activating and/or managing at least one Personal Security Device PSD (2040) with at least a first Remote Computer System (2050) over a first network (2045) using at least one Client (2010) as a host to said at least one PSD (2040), said method comprising the steps of:- a) establishing at least one communications pipe (2075) over said first network (2045) between said at least one PSD (2040) and said at least first Remote Computer System (2050),- b) retrieving proprietary information (I) by said at least first Remote Computer System (2050) from a remote storage location (2165),- c) transmitting said proprietary information (I) from said at least first Remote Computer System (2050) to said at least one PSD (2040) through said at least one communications pipe (2075), and- d) storing and/or processing said proprietary information (I) in said at least one PSD (2040).

WO 02/091316 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND SYSTEM FOR REMOTE ACTIVATION AND MANAGEMENT OF PERSONAL SECURITY DEVICES

1. Field of Invention

The present invention relates to a data processing method and system for remote activation and management of Personal Security Devices (PSD) over a network for purposes of obtaining services or data from one or more Remote Computer Systems. More particularly, the invention relates to a secure single-step method of activating and managing a Personal Security Device.

2. Background of Invention

The current art involving the management of Personal Security Devices (PSD), for example, smart cards, requires a multi-step process where all the information necessary to use a PSD is loaded into this PSD prior to distribution, including an initial Personal Identification Number or PIN. The PSD is then sent to the end user followed by a separate letter containing the initial PIN which the user must enter the first time the PSD is used. Another current alternative affixes an adhesive label containing a telephone number on a PSD prior to issuance. This label provides instructions for the end user to telephone a call center to activate the PSD before the device can be used.

The latter and former methods constitute multi-step processes, which adds considerably to the initial distribution and subsequent management costs of the PSDs. For example, in issuing smart cards, additional equipment, maintenance, labor and operating costs are required to generate either the separate mailings containing an initial PIN, or to generate adhesive labels to be placed on the smart cards and to operate the call centers which activate the cards.

Another major drawback of the current art concerns the lack of ability to manage information contained within the PSD after the device is issued. Currently, PSDs, which require changes, are either sent back to a central location or simply discarded and replaced with a new device. Both processes are time consuming and costly.

3. Summary of Invention

It is an object of the present invention to provides a post-issuance method for securely downloading and managing information inside the protected domain of a PSD.

This object is achieved with a method for activating and/or managing at least one PSD with at least a first Remote Computer System over a first network using at least one Client as a host to said at least one PSD, said method comprising the steps of:

- a) establishing at least one communications pipe over said first network between said at least one PSD and said at least first Remote Computer System,
- b) retrieving proprietary information by said at least first Remote Computer System from a remote storage location,
- c) transmitting said proprietary information from said at least first Remote Computer System to said at least one PSD through said at least one communications pipe, and
- d) storing and/or processing said proprietary information in said at least one PSD.

This improvement over the current art utilizes a communications pipe which allows downloading of information into a blank PSD and subsequently managing that information. For purposes of this invention, a blank PSD lacks proprietary algorithms and/or data but does contain an embedded runtime environment and optionally a unique identifier code.

In a first embodiment of the method of the invention, said remote storage location is in said at least first Remote Computer System.

In a second embodiment of the method of the invention, said remote storage location is in an at least one subsequent Remote Computer System functionally connected to said at least first Remote Computer System over a second network, and said step b) comprises the step of transmitting said proprietary information from said at least one subsequent Remote Computer System to said at least first Remote Computer System through said second network.

These embodiments allow either the Remote Computer System maintaining the communications pipe (first embodiment) or a subsequent Remote Computer System (second embodiment) to download proprietary information such as authentication algorithms, cryptographic keys, credentials or certificates directly into a PSD connected to a local Client through the communications pipe without disclosing proprietary information to the local Client.

A major advantage of the method of the invention is that it allows blank PSDs to be issued in bulk and activated at a future date without risk of compromise. Since no proprietary data is included in a bulk distribution, the PSDs are not usable to gain access to secure functions or data.

An example process by which a blank PSD becomes activated is as follows; an end user, who has previously received a blank PSD, connects the PSD to a local Client and accesses a predetermined site over a network located on a Remote Computer System. The Remote Computer System may optionally perform end user authentication by some predetermined method such as prompting for a social security number, static PIN, mother's maiden name, etc. Alternatively, authentication may be implied using a unique identifier contained within the PSD.

Once the end user is properly authenticated or valid PSD connected, a Remote Computer System forms a communications pipe and downloads (first embodiment), or causes a subsequent Remote Computer System to download (second embodiment), the necessary information through the communications pipe and into the PSD. The PSD may become activated upon completion of the process or as an additional security measure, the end user is prompted to devise and enter a unique PIN code to further protect access to the PSD.

In both said embodiments of the invention, a means to manage (e.g. upgrade, change, delete) PSD algorithms and data is facilitated by remotely gaining access to the PSDs and then downloading the changes directly into the PSDs, again without leaving proprietary information on the Clients. Any changes necessary to proprietary information may be performed entirely within the secure domain of the PSD.

In both said embodiments of the invention, all transactions occur within the secure domain of a PSD and a secure remote computer system, thus providing end-to-end security.

In said second embodiment of the invention, a centralized depository for tracking of PSD changes is provided, which greatly simplifies the management of large numbers of PSDs.

It is another object of the invention to provide a system for implementing the above-mentioned method.

4. Brief Description of Drawings

FIG. 1 is a generalized system block diagram for implementing a plain communications pipe,

FIG. 2 is a detailed block diagram depicting initiating a plain communications pipe,

FIG. 3 is a detailed block diagram depicting establishing a plain communications pipe,

FIG. 4A is a generalized system block diagram for implementing a secure communications pipe which includes software-based security mechanisms,

FIG. 4B is a generalized system block diagram for implementing a secure communications pipe which includes HSM-based security mechanisms,

FIG. 5 is a detailed block diagram depicting initiating a secure communications pipe,

FIG. 6 is a detailed block diagram depicting establishing a secure communications pipe,

FIG. 7 is a general system block diagram for implementing the authentication of a PSD vis-à-vis at least one Remote Computer System,

FIG. 8 is a detailed block diagram illustrating initial authentication challenge,

FIG. 9 is a detailed block diagram illustrating initial authentication response,

FIG. 10 is a detailed block diagram illustrating remote authentication challenge,

FIG. 11 is a detailed block diagram illustrating remote authentication response,

FIG. 12 is a detailed block diagram illustrating authentication credential transfer,

FIG. 13 is a detailed block diagram illustrating remote authentication challenge using said transferred credential,

FIG. 14 is a detailed block diagram illustrating remote authentication response using said transferred credential,

FIG. 15A is a general system block diagram for implementing present invention using a first Remote Computer System (first embodiment of the invention),

FIG. 15B is a general system block diagram for implementing present invention using a subsequent Remote Computer System (second embodiment of the invention),

FIG. 16 is a detailed block diagram illustrating the direct transfer of proprietary information to a PSD (first embodiment of the invention),

FIG. 17 is a detailed block diagram illustrating the remote transfer of proprietary information to a PSD (second embodiment of the invention).

5. Detailed Description of the Invention

In a first part (section 5.1.), the present Detailed Description of the Invention will disclose how to establish a plain communications pipe and a secure communications pipe between a PSD and a Remote Computer System.

In a second part (section 5.2.), the present Detailed Description of the Invention will disclose how to enhance security of an authentication process of a PSD vis-à-vis a Remote Computer System using said secure communications pipe, and how to use said Remote Computer System as a secure hub for authentication of said PSD vis-à-vis a plurality of subsequent Remote Computer Systems.

In a third part (section 5.3.), the present Detailed Description of the Invention will disclose a post-issuance method and system for securely downloading and managing information inside the protected domain of a PSD.

Said second part of the Detailed Description will be based on the use of a secure communications pipe, but the present invention is not limited to such a use.

The use of a plain communications pipe, i.e. of a communications pipe which does not involve end-to-end cryptographic mechanisms, falls within the scope of the present invention.

Note also that the following description of the invention will be based on a PSD which receives and sends APDU-(Application Protocol Data Unit)-formatted messages.

APDU messaging format, which is *per se* known in the art, is a lower-level messaging format which allows a PSD to communicate with higher-level applications located in devices to which the PSD is to be connected.

It must be clear that the present invention is not limited to the use of an APDU messaging format, and that any other low-level messaging format that can be processed by the PSD enters within the scope of the present invention.

5.1. Establishment of a Communications Pipe

5.1.1. Plain Communications Pipe

Referring to FIG. 1, a generalized system block diagram of the architectures of a Client 10 and of a Remote Computer System is depicted. The various layers shown are based on the Open System Interconnection model (OSI). For simplicity, certain layers common to both the Client and Remote Computer System are not shown and should be

assumed to be present and incorporated into adjacent layers. The layers common to both a Client and Remote Computer System include:

- an Applications Layer 90 which generally contains higher level software applications (e.g. word processor) and a user interface and such as a Graphical User Interface (GUI),

- an Applications Programming Interface ~~level~~ (API) Layer 100 for processing and manipulating data for use by either higher or lower level applications,

- a Communications Layer 105 which contains communications programs including secure communications capabilities, which enable a Client to communicate with a Remote Computer System to exchange information in an agreed upon protocol and visa versa,

- an Operating System Layer 110 or equivalent runtime environment, which controls the allocation and usage of hardware resources such as memory, Central Processing Unit (CPU) time, disk space, hardware I/O port assignments, peripheral device management,

- a Hardware Drivers Layer 120 which permits the operating system to communicate and control physical devices connected to the Client's or Remote Computer System's hardware I/O bus,

- and a Physical Device Layer 130 where Network Interface Cards (NIC) 140 provide the physical connections to a telecommunications network 45. Other Hardware Devices 80 may also be connected at this Layer.

5.1.1.1. Client Specific Features

A specialized program contained within the API Layer 100 of the Client and referred to as a Pipe Client 15, interacts with Communications Programs contained within the Communications Layer 105. The Pipe Client 15 functions to separate encapsulated APDU requests from incoming messaging packets received from a network 45 for processing by a locally connected PSD 40. Alternately, outbound APDU responses generated by a locally connected PSD 40, are processed by the Pipe Client for

encapsulation into an agreed upon communications protocol by Communications Programs contained within the Communications Layer 105.

A software driver contained within the Communications Layer 105 of the Client and referred to as a PSD Software Interface 20 directs incoming APDUs communicated by the Pipe Client 15 into the I/O device port connecting the PSD Hardware Device Interface 25 to the locally connected PSD 40. Outgoing APDUs generated by the PSD are communicated through the PSD Hardware Device Interface 25 through the I/O device port to the PSD Software Interface 20 and subsequently communicated to the Pipe Client 15.

5.1.1.2. Remote Computer System Specific Features

A first specialized program contained within the API Layer 100 of the Remote Computer System 50 and referred to as an APDU Interface 55, translates higher level messaging formats into low-level APDU messaging format required to communicate with a PSD 40. Alternately, the APDU Interface 55 translates incoming APDU responses received from a PSD 40 into higher level messaging formats used by programs in the API Layer 100 and Applications Layer 90 of the Remote Computer System.

A second specialized program contained within the API Layer 100 of the Remote Computer System 50 and referred to as a Pipe Server 70 interacts with Communications Programs contained within the Communications Layer 105. The Pipe Server 70 functions to separate encapsulated APDU requests from incoming messaging packets received from a network 45 for processing by the APDU Interface 55. Alternately, outbound APDU requests translated by the APDU Interface 55 are processed by the Pipe Server for encapsulation into an agreed upon communications protocol by Communications Programs contained within the Communications Layer 105.

5.1.1.3. Other Features

The connection 30 between the PSD 40 and PSD Hardware Interface 25 includes but is not limited to traditional electrical or optical fiber connections or wireless means including optical, radio, acoustical, magnetic, or electromechanical. Likewise the connection 75 between the Client 10 and the network 45, and the connection 75 between the Remote Computer System 50 and the network 45 may be accomplished analogously.

The network, shown generally at 45, includes both public and private telecommunications networks connected by traditional electrical, optical, electro-acoustical (DTMF) or by other wireless means. Any mutually agreed upon

communications protocol capable of encapsulating APDU commands may be employed to establish a plain communications pipe including open or secure communications protocols.

Referring now to FIG. 2, depicts initiating a plain communications pipe between the Remote Computer System 50 and the PSD 40 connected to a Client 10. In this depiction, the Remote Computer System 50 is sending a request to PSD 40 for non-proprietary embedded information 35, for example an identification number. PSD 40 is connected 30 to the local Client 10 using PSD Interface 25. PSD Interface 25 communicates with the Client 10 via hardware device port 5.

To initiate a plain communications pipe between Remote Computer System 50 and PSD 40, the Remote Computer System 50 generates a request 200 by way of API programs 100 which is translated into APDU format 220 by the APDU Interface 55 and sent to the Pipe Server 70 for message encapsulation. The encapsulated APDUs are then sent 210 to the Communications Programs 105S for incorporation into outgoing message packets 230.

The message packets 230 containing the encapsulated APDUs are transmitted 75 over the network 45 via a Network Interface Card (I/O) 130S. The Client 10 receives the message packets 240 containing the encapsulated APDUs which are received from the network 45 via a Network Interface Card (I/O) 130C installed on the local Client. The incoming messages are processed by Client-side Communications Programs 105C and routed 250 into the Pipe Client 15 for APDU extraction. The extracted APDUs are sent 260 through hardware device port 5, routed 270 into the PSD Interface 25 and sent to PSD 40 via connection 30 for processing within PSD domain 35.

Alternative requests to form a plain communications pipe 75 between a Remote Computer System 50 and a PSD 40 may be initiated by Client 10 requesting access to information contained on one or more networked local Clients, by connecting a PSD 40 to PSD Interface 25 which initiates a request to form a plain communications pipe 75, or by another Remote Computer System requesting access to PSD 40.

Referring now to FIG. 3, depicts a PSD response which establishes the plain communications pipe between PSD 40 and Remote Computer System 50. In this depiction, the request previously received is processed within the PSD domain 35, which generates a response message. The PSD response is sent in APDU format from PSD 40 through connection 30 and into PSD interface 25. The PSD response is then routed 370 through hardware device port 5 and sent 360 to the Pipe Client 15 for processing and encapsulation. The resulting message packets are then sent 350 to the Client-side Communications Programs 105C for incorporation into outgoing message packets 340.

The message packets 340 containing the encapsulated APDUs are transmitted 75 over the network 45 via the Network Interface Card (I/O) 130C.

The Remote Computer System 50 receives the message packets 330 containing the encapsulated APDUs, which are received from the network 45 via the Network Interface Card (I/O) 130S installed on the Remote Computer System. The incoming messages are processed by server-side Communications Programs 105S and routed 310 into the Pipe Server 70 for APDU extraction. The extracted APDUs are sent 320 to the APDU Interface 55 for processing and translation into a higher-level format and sent 300 to API Level programs 100 for processing and further transactions with the PSD 40 if desired.

5.1.2. Secure communications pipe

Referring now to FIG. 4A, a generalized system block diagram of one implementation of a secure communications pipe is shown. The general system block diagram includes an additional software-based Cryptography Module 470 installed on the Remote Computer System, which is not shown in FIG. 1.

FIG. 4B depicts an alternative to using software-based security mechanisms. In this alternative, a Hardware Security Module (HSM) 440 is employed to perform cryptographic functions. To access the HSM, a software driver referred to as an HSM S/W Interface 475, is included in the API Layer 100. The HSM software driver communicates with a physical device interface included in the Physical Device Layer 130. The physical device interface is installed on the I/O bus of the Remote Computer System, and is referred to as an HSM H/W Interface 485. The HSM module 440 is connected 430 to the HSM H/W Interface in a manner analogous to the PSD connection to the PSD Interface previously described. The use of HSM technologies provides end-to-end security, which further reduces the possibility of unauthorized disclosure of cryptographic or sensitive information.

Both APDU messaging security mechanisms shown in FIGs. 4A & 4B are used to generate cryptographic keys necessary to unlock secure functions and data contained within the secure domain of a PSD, encrypt outgoing APDUs and decrypt incoming encrypted APDUs. The security mechanisms employed in generating a secure pipe may include synchronous, asynchronous or any combination of cryptography methods.

Secure communications protocols used to communicate over a network are accomplished by the Communications Programs contained within the Communications Layers 105. Cryptography used in generating secure communications may employ the

security mechanisms described for APDU messaging, employ separate mechanisms or employ any combination thereof.

Referring now to FIG. 5, depicts the initiating of a secure pipe between the Remote Computer System and the PSD 40 connected to Client 10. In this depiction, Remote Computer System 50 is sending a secure request to PSD 40 for proprietary embedded information 35, for example an authentication password. PSD 40 is connected 30 to the local Client 10 using PSD Interface 25. PSD Interface 25 communicates with the Client 10 via hardware device port 5.

To initiate a secure communications pipe between Remote Computer System 50 and PSD 40, a request 500 is generated on Remote Computer System 50 to access PSD 40 by way of API programs 100 which are translated into APDU format by the APDU Interface 55. The APDUs are then sent 520 to a Security Module 525 for encryption using a pre-established cryptography method. The proper cryptographic parameters may be determined by using a look-up table or database, which cross-references the PSD's unique internal identification information with one or more codes necessary to implement the appointed cryptography method.

The encrypted APDUs are then routed 510 to the Pipe Server 70 for message encapsulation. The encapsulated APDUs are then sent 530 to the Communications Programs 105 for processing, encryption using a pre-established secure communications protocol and incorporation into outgoing message packets 535. The secure message packets 535 containing the encrypted and encapsulated APDUs are transmitted 75 over the network 45 via a Network Interface Card (I/O) 130S.

The Client 10 receives the message packets 540 containing the encrypted and encapsulated APDUs which are received from the network 45 via a Network Interface Card (I/O) 130C installed on the local Client 10.

The incoming encrypted message packets are decrypted and processed using the pre-established cryptography employed in the secure communications protocol by Client-side Communications Programs 105C. The unencrypted message packets still containing the encrypted APDUs are routed 550 into the Pipe Client 15 for APDU extraction. The extracted APDUs are sent 560 through hardware device port 5, routed 570 into the PSD Interface 25 and sent to PSD 40 via connection 30 for decryption and processing within the secure domain 35 of the PSD 40. Using a pre-established cryptography method, incoming secure APDUs are decrypted and requests processed.

Referring now to FIG. 6, depicts a PSD secure response, which establishes the secure communications pipe between PSD 40 and Remote Computer System 50. In this depiction, the secure request previously received is processed within the secure domain

35 of the PSD 40, which causes the PSD to generate a secure response message using a pre-established cryptography method.

The PSD secure response is sent in APDU format from PSD 40 through connection 30 and into PSD interface 25. The PSD secure response is then routed 670 through hardware device port 5 and sent 660 to the Pipe Client 15 for processing and encapsulation. The resulting message packets are then sent 650 to the Client-side Communications Programs 105 for processing, encryption using a pre-established secure communications protocol and incorporation into outgoing message packets 640. The message packets 640 containing the encapsulated APDUs are transmitted 75 over the network 45 via the Network Interface Card (I/O) 130C.

The Remote Computer System 50 receives the message packets 635 containing the encapsulated APDUs from the network 45 via the Network Interface Card (I/O) 130S installed on the Remote Computer System 50. The incoming messages are processed and decrypted using the pre-established cryptography method employed in the secure communications protocol by the server-side Communications Programs 105 and routed 610 into the Pipe Server 70 for secure APDU extraction. The extracted secure APDUs are sent 630 to the Security Module 525 for decryption of the secure APDUs using the pre-established cryptography method. The decrypted APDUs are then routed 620 to the APDU Interface 55 for processing and translation into a higher-level format and sent 600 to API programs 100 for processing and further transactions with the PSD 40 if desired. This step establishes the secure "pipe" to communicate with the PSD. The secure pipe is maintained until the Remote Computer System signals the Client to close the hardware interface port 5.

No limitation is intended in the number of PSDs and Clients forming communications pipes 75 with one or more Remote Computer System(s) 50, nor should any limitation on the number of Remote Computer Systems 50 available for generating communications pipes 75 be construed from the drawings. Lastly, no limitation is intended concerning the initiating event to establish a communications pipe.

5.2. Authentication method using a communications pipe

As already mentioned above, description of said authentication method will be based on the use of a secure communications pipe, but the present invention is not limited to such a use.

The use of a plain communications pipe falls within the scope of the present invention.

The steps involved in performing authentication through a secure communications pipe are shown in Figures 7 through 14. Figure 7 is a generalized system block diagram. Figures 8 through 11 illustrate a first variant where responses to authentication challenges are generated within the secure domain of a Personal Security Device. Figures 12 through 14 illustrate a second variant where a Remote Computer System acting as a secure hub provides the proper response to authentication challenges, rather than directing challenges through the communications pipe into the PSD for processing. Characters shown with a prime sign (e.g. C') indicate a duplicate of an original authentication credential. Other drawing details shown but not described refer to information described in previous section 5.1.

Referring now to FIG. 7, a generalized system block diagram is depicted, where a Personal Security Device 1040 is connected to a Client 1010 which is itself connected over a network 1045 to a Remote Computer System 1050 using a secure communications pipe 1075 as described in previous section 5.1.2. Remote Computer System 1050 is operating as a secure hub following initial authentication as described below, to service authentication requests made by subsequent Remote Computer Systems sent over a network 1045 or 1045A.

The subsequent Remote Computer System 1150 is an example of a system requiring authentication when a request for secure functions or data is sent from Client computer 1010 over the networks 1045 and 1045A. The secure communications pipe 1075 applies to authentication transactions but does not restrict nor control non-secure transactions occurring over either network 1045 or 1045A.

Networks 1045 and 1045A may be a common network as in a virtual private networking arrangement or separate networks such as private intranet and public internet arrangements. The networks 1045 and 1045A are depicted separately for illustrative purposes only. No limitation is intended in the number of PSDs and Clients forming communications pipes 1075 with one or more secure hubs 1050; nor should any limitation on the number of subsequent Remote Computer Systems 1150 available for authentication be construed from the drawing. Transactions not involving authentications are not restricted to the secure hub.

The basic operation of the secure hub may be initiated when an end user at a Client requests access to secure functions or data contained on one or more Remote Computer Systems connected by a network. An available Remote Computer System, in which a secure communications pipe has been established as described in previous section 5.1.2., authenticates the end user and Client using the security mechanisms contained within the secure domain of the PSD. Alternatively, an external event such as a

need to update information within a PSD may trigger a subsequent Remote Computer System to initiate the authentication process.

Once an initial Client authentication has been accomplished by the available Remote Computer System, subsequent authentication challenges transmitted over a network 1045 or 1045A made by subsequent Remote Computer Systems are directed to the Remote Computer System 1050 acting as a secure hub and depending on which variant employed, are either routed through the appropriate communications pipe 1075 to PSD 1040 or are directly authenticated by the Remote Computer System 1050.

5.2.1. First variant of authentication method

Referring to FIG. 8, to establish a secure hub, a Client 1010 causes an authentication challenge to be generated on a Remote Computer System 1050, by requesting access to secure functions or data over a network 1045. Upon receiving the request from Client 1010, the Remote Computer System 1050 generates an authentication challenge 1205 within a secure domain designated as authentication routine 1065. The authentication challenge is processed by an API level program 1100 and routed 1200 to an APDU interface 1055 for translation into an APDU format. The APDUs are then sent 1220 to a Security Module 1225 for encryption. The encrypted APDUs are then routed 1230 to a Pipe Server 1070 for encapsulation into outgoing messaging and sent 1210 to the Communications Programs 1105S for transmission over the communications pipe 1075, through the network 1045 into the network interface 1130C of the Client 10. The incoming messages are then routed 1240 to Communications Programs 1105C for processing.

Following processing, the messages are sent 1250 to a Pipe Client 1015 for separation of the encapsulated APDUs. The APDUs are then sent 1260 through a hardware device port 1005 assigned to a PSD Interface 1025. PSD Interface 1025 routes the incoming APDUs into the PSD 1040 via connection 1030, where it is subsequently decrypted and processed within its secure domain 1035.

Referring to FIG. 9, once PSD 1040 has processed the authentication challenge within the secure domain 1035 of the PSD, an authentication response message is generated using a pre-established cryptography method.

The authentication response is sent in APDU format from PSD 1040 through connection 1030 and into PSD interface 1025. The PSD secure response is then routed 1370 through hardware device port 1005 and sent 1360 to the Pipe Client 1015 for processing and encapsulation. The resulting message packets are then sent 1350 to the

Client-side Communications Programs 1105C for processing, encryption using a pre-established secure communications protocol and incorporation into outgoing message packets 1340. The message packets 1340 containing the encapsulated APDUs are transmitted 1075 over the network 1045 via a network interface card (I/O) 1130C.

The Remote Computer System 1050 receives the message packets 1335 containing the encapsulated APDUs from the network 1045 via a network interface card (I/O) 1130S installed on the Remote Computer System. The incoming messages are processed and decrypted using the pre-established cryptography method employed in the secure communications protocol by the server-side Communications Programs 1105S and routed 1310 into the Pipe Server 1070 for secure APDU extraction. The extracted secure APDUs are sent 1330 to the Security Module 1325 for decryption of the secure APDUs using the pre-established cryptography method. The decrypted APDUs are then routed to the APDU Interface 1055 for processing and translation into a higher-level format and sent 1300 to API Level programs 1100 for processing. If authentication is successful, the Remote Computer System 1050 allows access to secure functions or data and establishes itself as a secure hub. If authentication fails, the end user will be unable to access secure functions or data.

Referring to FIG. 10, once the secure hub has been established as previously described, remote authentication of subsequent Remote Computer Systems may be accomplished. Remote authentication may be initiated either by a Client's request for access to secure functions or data or by other Remote Computer Systems to perform transactions within the secure domain of a PSD.

To perform a remote authentication, a challenge 1085 is issued by a subsequent Remote Computer System 1150. The challenge is routed over a network 1045, into the secure hub 1050. The incoming challenge is processed and decrypted in the secure hub 1050 using the pre-established cryptography method employed in the secure communications protocol by the server-side Communications Programs 1105S and routed 1085 to an API level program 1100 where it is processed and routed 1400 to an APDU interface 1055 for translation into an APDU format. The APDUs are then sent 1420 to a Security Module 1425 for encryption. The encrypted APDUs are then routed 1430 to a Pipe Server 1070 for encapsulation into outgoing messaging and sent 1410 to the communications programs 1105S for transmission over the communications pipe 1075, through the network 1045 into the network interface 1130C of the Client 1010.

The incoming messages are then routed 1440 to Communications Programs 1105C for processing. Following processing, the messages are sent 1450 to a Pipe Client 1015 for separation of the encapsulated APDUs. The APDUs are then sent 1460

through a hardware device port 1005 assigned to a PSD Interface 1025. PSD Interface 1025 routes the incoming APDUs into the PSD 1040 via connection 1030, where it is subsequently decrypted and processed within its secure domain 1035.

Referring to FIG. 11, once PSD 1040 has processed the authentication challenge within its secure domain 1035, an authentication response message is generated using a pre-established cryptography method. The authentication response is sent in APDU format from PSD 1040 through connection 1030 and into PSD interface 1025. The PSD secure response is then routed 1570 through hardware device port 1005 and sent 1560 to the Pipe Client 1015 for processing and encapsulation. The resulting message packets are then sent 1550 to the Client-side Communications Programs 1105C for processing, encryption using a pre-established secure communications protocol and incorporation into outgoing message packets 1540. The message packets 1540 containing the encapsulated APDUs are transmitted 1075 over the network 1045 via network interface card (I/O) 1130C.

The secure hub 1050 receives the message packets 1535 containing the encapsulated APDUs from the network 1045 via network interface card (I/O) 1130S. The incoming messages are processed and decrypted using the pre-established cryptography method employed in the secure communications protocol by the server-side Communications Programs 1105S and routed 1510 into the Pipe Server 1070 for secure APDU extraction. The extracted secure APDUs are sent 1530 to the Security Module 1525 for decryption of the secure APDUs using the pre-established cryptography method. The decrypted APDUs are then routed 1520 to the APDU Interface 1055 for processing and translation into a higher-level format and sent 1500 to API Level programs 1100 for processing. Authentication Module 1065 within the secure hub 1050 remains inactive during the transfer of authentication information. The authentication response message is then routed 1085 into the Communications Programs 1105S where the response is sent over the network 1045 in a pre-established secure communications protocol to the challenging subsequent Remote Computer System 1150.

The incoming response message is decrypted and sent to an Authentication Module 1095. If authentication is successful, the subsequent Remote Computer System 1150 allows access to secure functions or data. If authentication fails, the end user will be unable to access secure functions or data.

5.2.2. Second variant of authentication method

Referring to FIG. 12 depicts a second variant of the authentication method where the Remote Computer System 1050 transfers copies of the PSD credentials C 1035, if not pre-existing on said Remote computer System 1050. To perform credential transfer, an initial authentication transaction is performed by the Remote Computer System 1050 as previously described. Following authentication, additional commands are sent by the Remote Computer System 1050 to transfer the specified credentials.

The credentials are generated using a pre-established cryptography method and sent in APDU format from PSD 1040 through connection 1030 and into PSD interface 1025. The PSD secure response is then routed 1670 through hardware device port 1005 and sent 1660 to the Pipe Client 1015 for processing and encapsulation. The resulting message packets are then sent 1650 to the Client-side Communications Programs 1105C for processing, encryption using a pre-established secure communications protocol and incorporation into outgoing message packets 1640. The message packets 640 containing the encapsulated APDUs are transmitted 1075 over the network 1045 via a network interface card (I/O) 1130C.

The Remote Computer System 1050 receives the message packets 1635 containing the encapsulated APDUs from the network 1045 via network interface card (I/O) 1130S installed on the Remote Computer System.

The incoming messages are processed and decrypted using the pre-established cryptography method employed in the secure communications protocol by the server-side Communications Programs 1105S and routed 1610 into the Pipe Server 1070 for secure APDU extraction. The extracted secure APDUs are sent 1630 to the Security Module 1625 for decryption of the secure APDUs using the pre-established cryptography method. The decrypted APDUs are then routed 1620 to the APDU Interface 1055 for processing and translation into a higher-level format and sent 1600 to API Level programs 1100 for processing and subsequently sent 1605 to the Authentication Module 1065 for secure storage and future use. The transferred authentication information is shown in FIG. 12 as C'.

In FIG. 13, an authentication challenge 1085 is sent by a subsequent Remote Computer System 1150 over a network 1045. The Remote Computer System 1050 acting as a secure hub receives the incoming challenge 1085 from the network 1045 via network interface card 1130S installed on the Remote Computer System 1050. The incoming challenges 1085 are processed and decrypted using the pre-established cryptography method employed in the secure communications protocol by the server-side

Communications Programs 1105S and routed to API Level programs 1100 for processing. The processed challenge is then sent 1705 to the Authentication Module 1065 for authentication using the PSD's transferred credentials C' 1035'. The communications pipe 1075 may remain intact during this process to allow for other transactions to occur.

Referring to FIG. 14, the secure hub 1050 generates an authentication reply within the Authentication Module 1065 which is sent 1805 to the API Level Programs 1100 for processing, and subsequently routed 1810 to the Server-side Communications Programs 1105S for processing, encryption using a pre-established secure communications protocol and incorporation into outgoing message packets. The message packets are routed over the network 1045 to the challenging subsequent Remote Computer System 1150. The incoming messages are then decrypted and the authentication reply processed by an internal authentication module 1095. If authentication is successful, the subsequent Remote Computer System 1150 allows access to secure functions or data. If authentication fails, the end user will be unable to access secure functions or data.

5.3. Method and system for remote activation and management of PSDs

The need for secure network communications is paramount for sensitive business and government transactions. The present invention provides an improvement over the current art by allowing issuance of generic PSDs, which can be activated and customized at a later date.

The steps involved in activating a PSD and performing subsequent information management through a communications pipe are shown in FIG. 15 through 17. For purposes of demonstration, it should be assumed that any local authentications between the end user, Client and local network domain have already been accomplished. Preferentially, a secure communications protocol is employed over the network between the client and one or more Remote Computer Systems. It is understood to one skilled in the art, that either embodiment of the invention will work with or without the use of secure communications protocols.

Referring now to FIG. 15A, a first embodiment of the invention is depicted where a Client 2010 and a connected PSD 2040 are connected over a network 2045 with a Remote Computer System 2050 using a communications pipe 2075 as described in previous section 5.1. The Remote Computer System 2050 maintains the communications

pipe 2075 and is available to transfer proprietary information "I" 2165 through the communications pipe 2075 and into the PSD 2040.

In FIG. 15B, a second embodiment of the invention is depicted where a first Remote Computer System 2050 acting as a secure hub as described in previous section 5.2. provides a mechanism for a subsequent Remote Computer System 2150 connected 2085 to a network 2045 to transfer proprietary information "I'" 2165' into a PSD 2040. In this second embodiment of the invention, proprietary information 2165' is received and processed by a first Remote Computer System 2050. The proprietary information 2165' is then sent by the first Remote Computer System 2050, through the communications pipe 2075 and into the PSD 2040.

The network 2045 may be a common network as in a virtual private networking arrangement or separate networks such as private intranet and public internet arrangements. No limitation is intended in the number of PSDs 2040 and clients 2010 forming communications pipes 2075 with one or more Remote Computer Systems 2050, 2150; nor should any limitation on the number of Remote Computer Systems 2050, 2150 available for transferring proprietary information 2165, 2165' be construed from any of the depictions shown herein.

End user authentication is optional for activating blank PSDs or for deactivating PSDs already in use. In instances where access to a previously personalized PSD is desired, authentication transactions may be required as described in previous section 5.2. to facilitate secure access to the PSD. Once the authentication process has been accomplished, changes to proprietary information contained within the secure domain of the PSD are accomplished using the equivalent methodology described for blank card activation.

Proprietary information 2165, 2165' for injection into a PSD may originate on a Remote Computer system 2050 supporting a communications pipe (first embodiment of the invention), on subsequent Remote Computer Systems 2150 (second embodiment of the invention), or on any combination of Remote Computer Systems.

Referring to FIG. 16, this drawing illustrates the transfer of proprietary information from a storage location over a network into a PSD using the Remote Computer System supporting the communications pipe (first embodiment of the invention). This drawing is applicable for either activating a blank PSD or changing information in an active PSD subsequent to authentication. In this first embodiment of the invention, the proprietary information 2165 is called from its storage location 2160 within the Remote Computer System 2050.

After retrieval, the proprietary information 2165 is sent 2206 for processing into APDU format and encapsulation into the proper communications messaging format 2204 as described in previous section 5.1. After processing, the communications message 2204 is sent through the network interface 2130S, into the communications pipe 2075 over network 2045 and received by the client 2010 via a complementary network interface 2130C.

The incoming communications messages are sent 2212 for processing where the APDU formatted information is separated as described in previous section 5.1. The separated APDUs are then routed 2216 through the hardware device port 2005 and into 2218 the PSD device interface 2025. The incoming APDUs are then routed 2030 into the secure domain 2035 of the PSD 2040 where the information is processed and stored by at least one embedded algorithm.

For newly issued PSDs lacking proprietary information, the embedded algorithm is installed by the PSD issuer and functions to manage the initial installation of proprietary information. For PSDs already containing proprietary information, the algorithm may be the same or a different algorithm, which may include cryptographic capabilities.

Referring to FIG. 17, this drawing illustrates the transfer of proprietary information from a remote storage location 1160' over a network 2045 and injection into a PSD 2040 using a plurality of remote computer systems 2050, 2150. This second embodiment of the invention involves retrieving proprietary information 2165' from one or more 2150 remote computer systems, sending 2085 the proprietary information over a network 2045 where the proprietary information is received and processed by a first Remote Computer System 2050 which is supporting a communications pipe 2075 and injected into the secure domain 2035 of the PSD 2040.

This second embodiment of the invention is applicable for either activating a blank PSD or changing information in an active PSD subsequent to authentication. In instances where authentication is required, the Remote Computer System supporting the communications pipe may operate as a secure hub as described in previous section 5.2.

In this second embodiment of the invention, the proprietary information 2160' is called from a storage location inside a subsequent Remote Computer System 2150 or another Remote Computer System, which is local to, and communicating with, the subsequent Remote Computer System 2150. The proprietary information "I'" 2165' is retrieved and sent 2085 over the network 2045 to the Remote Computer System 2050 supporting the communications pipe 2075 with the designated PSD 2040.

Remote Computer System 2050 receives the proprietary information through the network interface 2130 and routes the incoming proprietary information 2165' for

processing it 2302 into APDU format and encapsulation into the proper communications messaging format 2304 as described in previous section 5.1. After processing, the message 2304 is sent through the network interface 2130S, into the communications pipe 2075 over network 2045 and received by the client 2010 via a complementary network interface 2130C.

The incoming communications messages are sent 2312 for processing in 2314 where the APDU formatted information is separated as described in previous section 5.1. The separated APDUs are then routed 2316 through the hardware device port 2005 and into 2318 the PSD interface 2025. The incoming APDUs are then routed 2030 into the secure domain 2035 of the PSD 2040 where the information is processed and stored by at least one embedded algorithm.

As previously described, for newly issued PSDs lacking proprietary information, the embedded algorithm is installed by the PSD issuer and functions to manage the initial installation of proprietary information. For PSDs already containing proprietary information, the algorithm may be the same or a different algorithm, which may include cryptographic capabilities.

The foregoing described embodiments of the invention are provided as illustrations and descriptions. They are not intended to limit the invention to precise form described. In particular, it is contemplated that functional implementation of the invention described herein may be implemented equivalently in hardware, software, firmware, and/or other available functional components or building blocks. Other variations and embodiments are possible in light of above teachings, and it is not intended that the scope of the invention be limited by this Detailed Description, but rather by the Claims following herein.

CLAIMS

What is claimed is :

1. A method for activating and/or managing at least one PSD (2040) with at least a first Remote Computer System (2050) over a first network (2045) using at least one Client (2010) as a host to said at least one PSD (2040), said method comprising the steps of:

- a) establishing at least one communications pipe (2075) over said first network (2045) between said at least one PSD (2040) and said at least first Remote Computer System (2050),

- b) retrieving proprietary information (I; I') by said at least first Remote Computer System (2050) from a remote storage location (2165; 2165'),

- c) transmitting said proprietary information (I; I') from said at least first Remote Computer System (2050) to said at least one PSD (2040) through said at least one communications pipe (2075), and

- d) storing and/or processing said proprietary information (I; I') in said at least one PSD (2040).

2. The method according to claim 1, further comprising the steps of:

- b1) encrypting said proprietary information (I; I') in said at least first Remote Computer System (2050) after said step b) and before said step c), and

- c1) decrypting said proprietary information in said at least one PSD (2040) after said step c) and before said step d).

3. The method according to claim 1 or 2, wherein said remote storage location (2165) is in said at least first Remote Computer System (2050).

4. The method according to claim 1 or 2, wherein said remote storage location (2165') is in an at least one subsequent Remote Computer System (2150) functionally-connected to said at least first Remote Computer System (2050) over a second network, wherein said step b) comprises the step of transmitting said proprietary information (I') from said at least one subsequent Remote Computer System (2165') to said at least first Remote Computer System (2050) through said second network.

5. The method according to claim 4, further comprising the steps of:

- encrypting said proprietary information (I') in said at least one subsequent Remote Computer System (2150), and

- decrypting said proprietary information (I') in said at least first Remote Computer System (2050).

6. The method according to claim 1 or 2, further comprising the step of authenticating said at least one PSD (2040) vis-à-vis said at least first Remote Computer System (2050) through said at least one communications pipe (2075) after said step a) and before said step b).

7. A Client (2010) for activating and/or managing at least one PSD (2040) with at least a first Remote Computer System (2050) over a first network (2045) using said Client (2010) as a host to said at least one PSD (2040), wherein said Client (2010) comprises means (2214) for transferring incoming and outgoing PSD-formatted messages between said at least one PSD (2040) and said at least first Remote Computer System (2050) through at least one communications pipe (2075) established over said first network (2045).

8. A Remote Computer System (2050) for activating and/or managing at least one PSD (2040) with said Remote Computer System (2050) over a first network (2045) using at least one Client (2010) as a host to said at least one PSD (2040), wherein said Remote Computer System (2050) comprises means for:

- storing proprietary information (I; I'), and for

- transmitting said proprietary information (I; I') to said at least one PSD (2040) through at least one communications pipe (2075).

9. The Remote Computer System (2050) according to claim 8, further comprising means for receiving said proprietary information from at least one subsequent Remote Computer System (2150) over a second network.

10. The Remote Computer System (2050) according to claim 8 or 9, further comprising cryptographic means for encrypting said proprietary information (I; I') before transmitting said proprietary information to said at least one PSD (2040) through said at least one communications pipe (2075).

11. A PSD activation and/or management system, comprising at least one Client (2010) according to claim 7 and at least a first Remote Computer System (2050) according to claim 8 functionally connected to said at least one Client (2010) through said at least one communications pipe (2075).

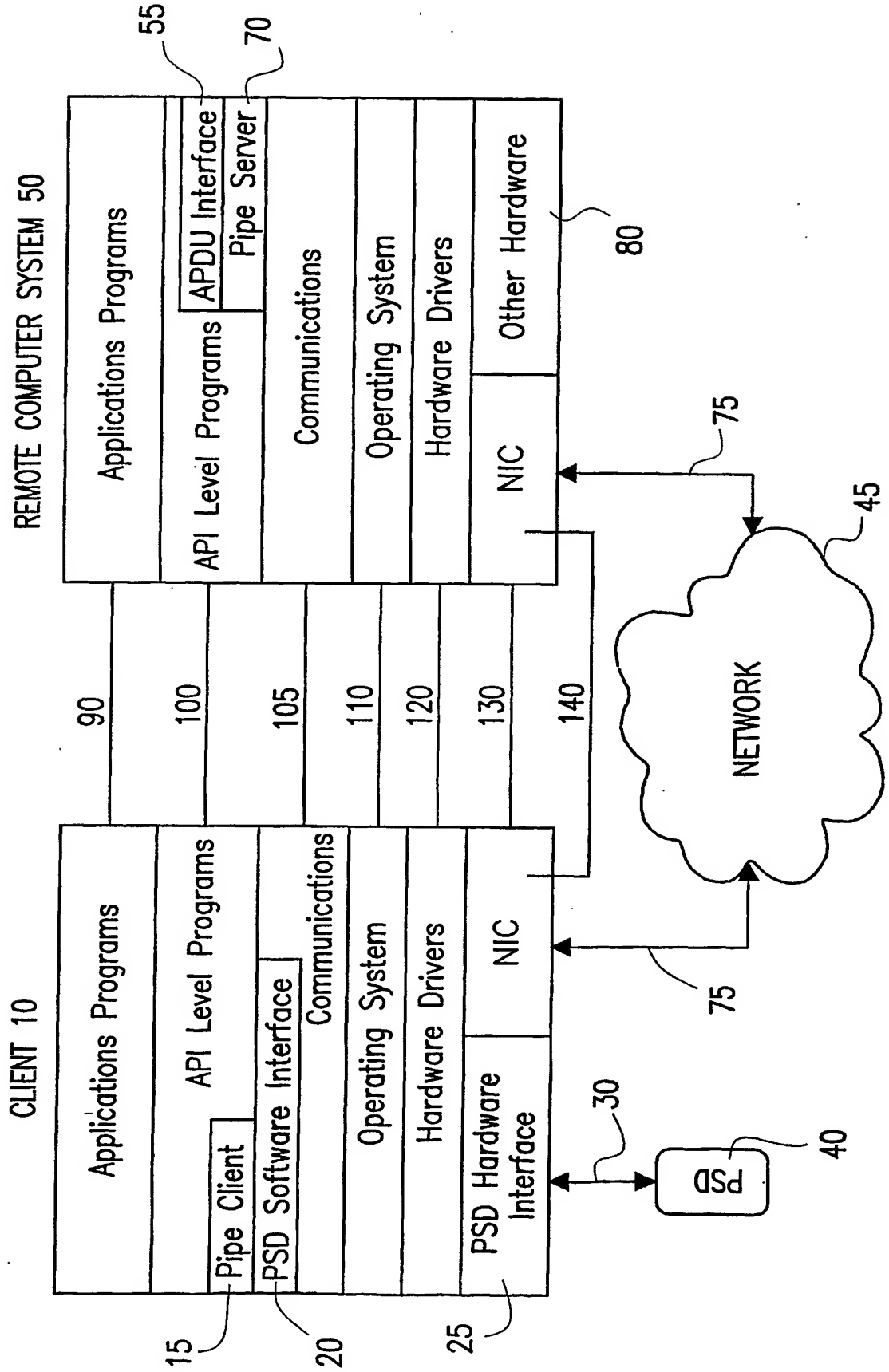
12. A PSD activation and/or management system, comprising at least one Client (2010) according to claim 7 and at least a first Remote Computer System (2050) according to claim 9 functionally connected to said at least one Client (2010) through said at least one communications pipe (2075).

13. The PSD activation and/or management system according to claim 12, further comprising said at least one subsequent Remote Computer System (2150) functionally connected to said at least first Remote Computer System (2050) through said second network, wherein said at least one subsequent Remote Computer System (2150) comprises means for transmitting said proprietary information to said at least first Remote Computer System (2050) through said second network.

14. The PSD activation and/or management system according to claim 13, wherein said at least one subsequent Remote Computer System (2150) comprises means for encrypting said proprietary information (I'), and wherein said at least first Remote Computer System (2050) comprises means for decrypting said proprietary information (I').

15. The PSD activation and/or management system according 13, wherein said first and second networks form one same network (2045).

FIG.1


REMOTE COMPUTER SYSTEM 50
Applications Programs
API Level Programs
APDU Interface
Pipe Server
Communications
Operating System
Hardware Drivers
NIC
Other Hardware
55
70
80
75
45
NETWORK
90
100
105
110
120
130
140
CLIENT 10
Applications Programs
API Level Programs
Pipe Client
PSD Software Interface
Communications
Operating System
Hardware Drivers
NIC
PSD Hardware Interface
15
20
25
30
PSD
40

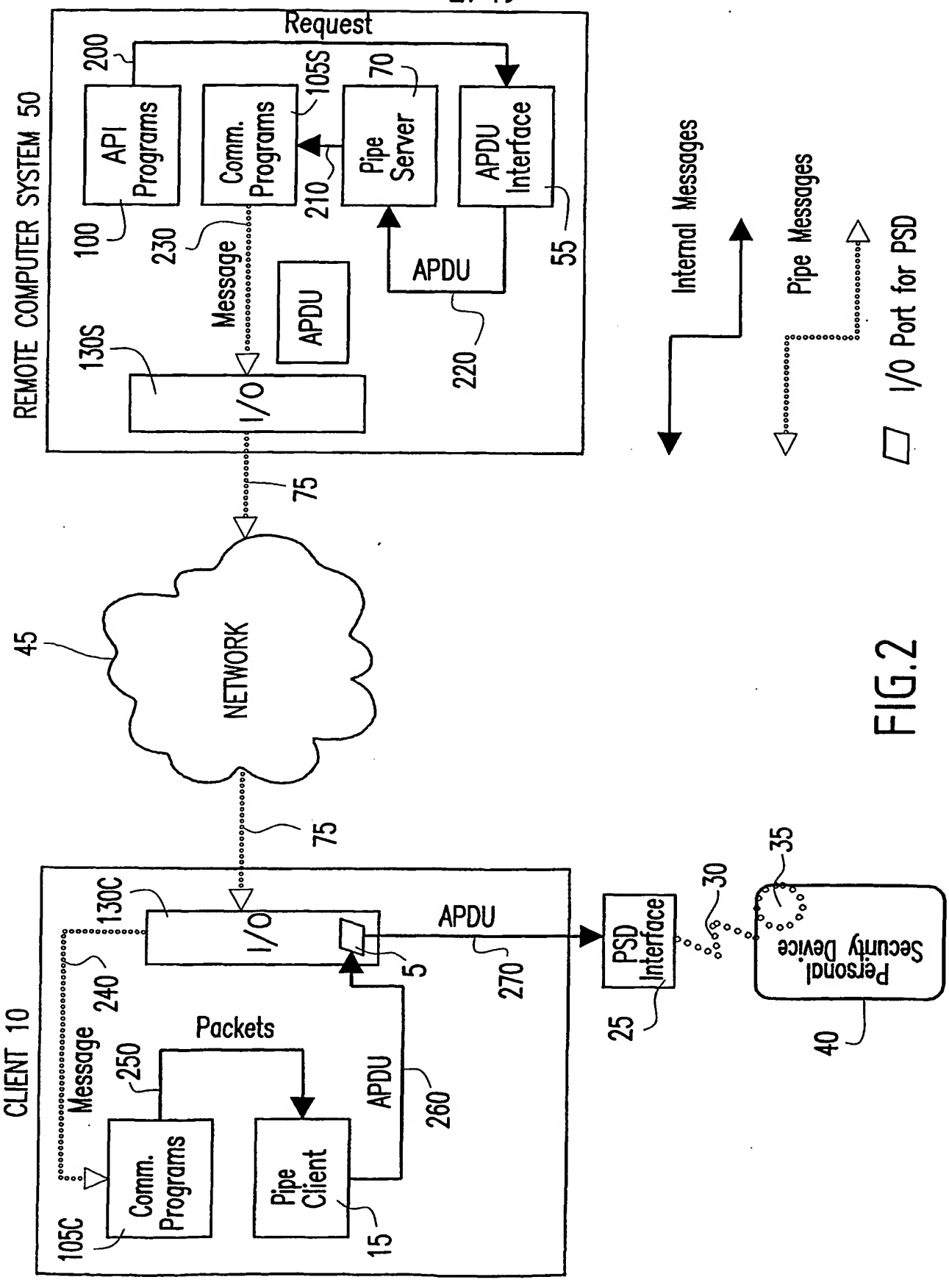

REMOTE COMPUTER SYSTEM 50
Request
200
API Programs
100
105S
Comm. Programs
230
210
70
Pipe Server
APDU Interface
55
Message
APDU
130S
I/O
220
APDU
75
45
NETWORK
75
CLIENT 10
130C
I/O
APDU
270
5
240
Message
Packets
250
APDU
260
105C
Comm. Programs
Pipe Client
15
PSD Interface
25
30
35
Personal Security Device
40
Internal Messages
Pipe Messages
I/O Port for PSD

FIG.2

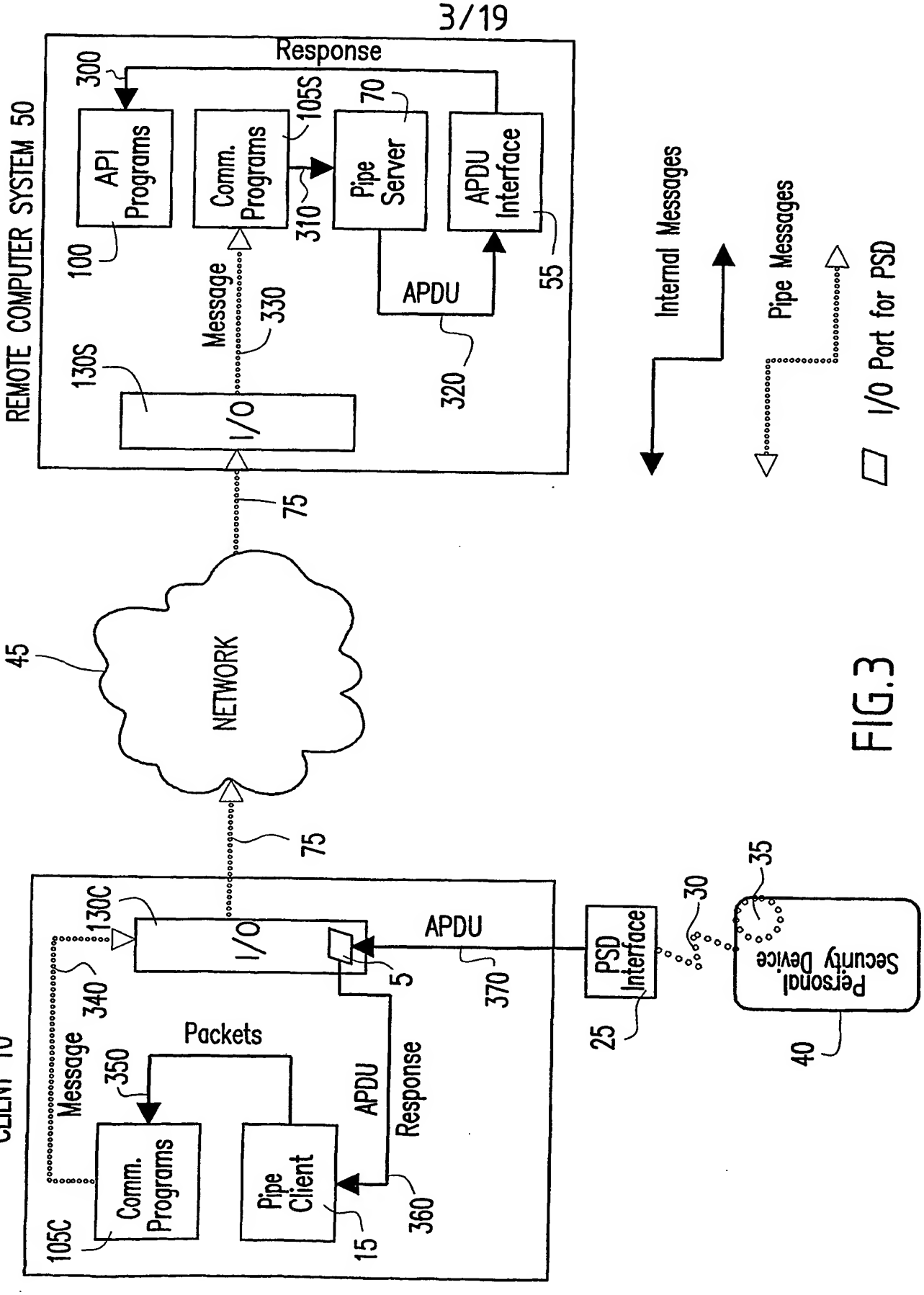

REMOTE COMPUTER SYSTEM 50
Response
300
API Programs
100
Comm. Programs
105S
310
Pipe Server
70
APDU Interface
55
Message
330
APDU
320
130S
I/O
75
NETWORK
45
75
CLIENT 10
130C
I/O
APDU
370
5
340
Packets
Message
350
Comm. Programs
105C
Pipe Client
15
APDU
Response
360
PSD Interface
25
30
35
Personal Security Device
40
Internal Messages
Pipe Messages
I/O Port for PSD

FIG.3

FIG.4A

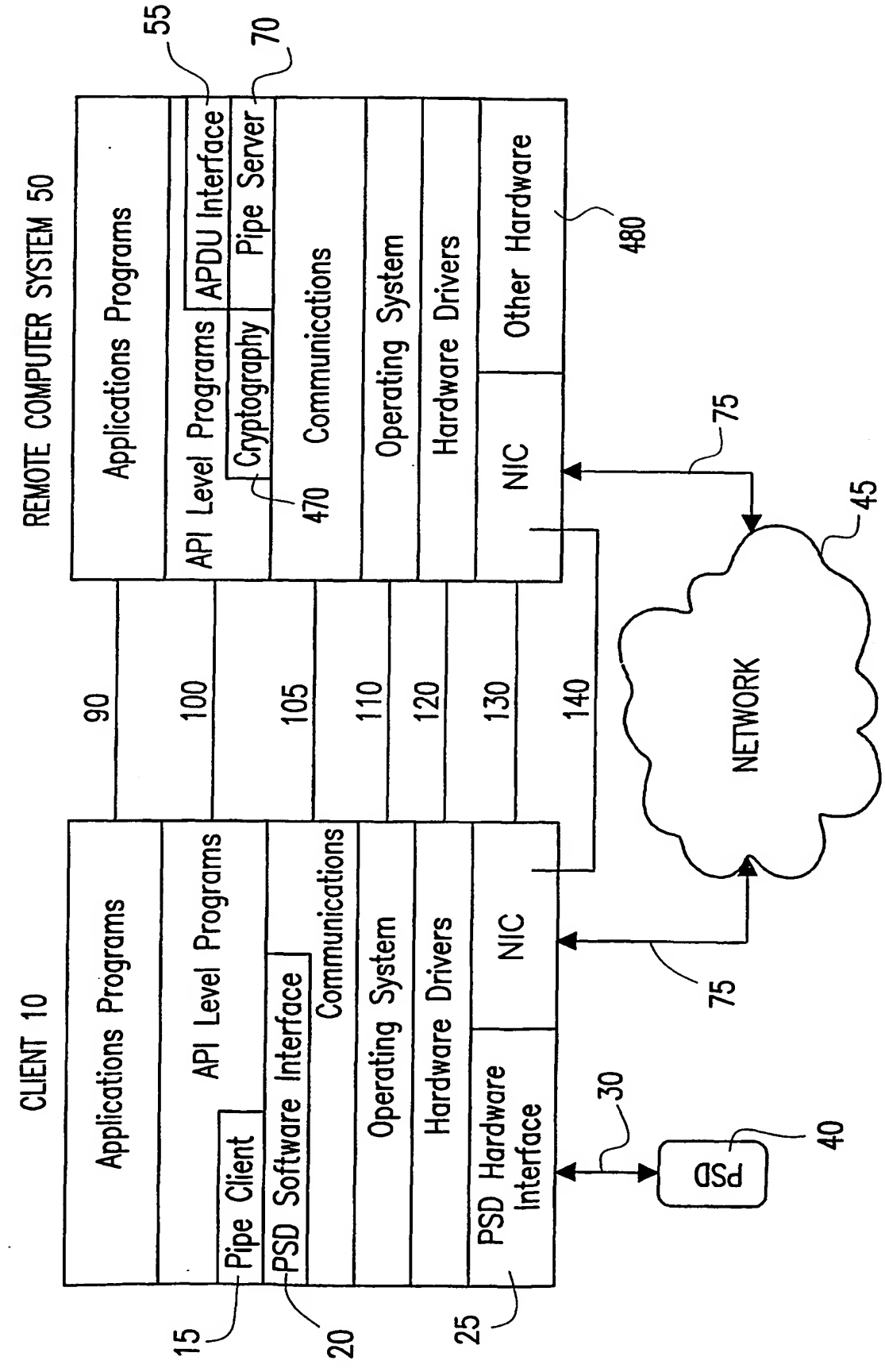
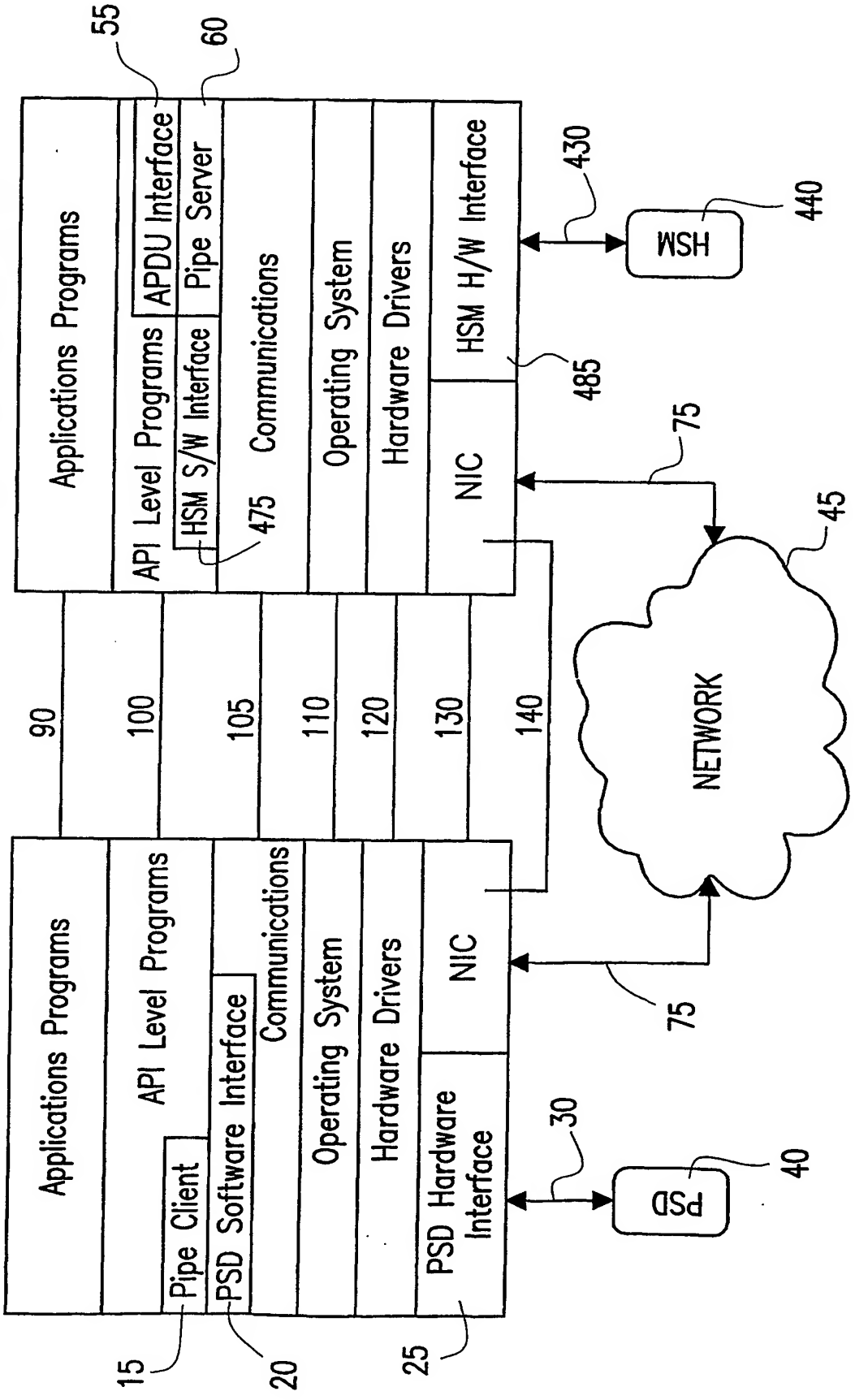

CLIENT 10
Applications Programs
API Level Programs
Pipe Client
PSD Software Interface
Communications
Operating System
Hardware Drivers
PSD Hardware Interface
NIC
15
20
25
30
40
PSD
75
NETWORK
45
75
REMOTE COMPUTER SYSTEM 50
Applications Programs
API Level Programs
APDU Interface
Cryptography
Pipe Server
Communications
Operating System
Hardware Drivers
NIC
Other Hardware
55
70
470
480
90
100
105
110
120
130
140

FIG.4B


CLIENT 10
Applications Programs
API Level Programs
Pipe Client
PSD Software Interface
Communications
Operating System
Hardware Drivers
PSD Hardware Interface
NIC
PSD
NETWORK
REMOTE COMPUTER SYSTEM 50
Applications Programs
API Level Programs
APDU Interface
HSM S/W Interface
Pipe Server
Communications
Operating System
Hardware Drivers
HSM H/W Interface
NIC
WSH
15
20
25
30
40
45
55
60
75
90
100
105
110
120
130
140
430
440
475
485

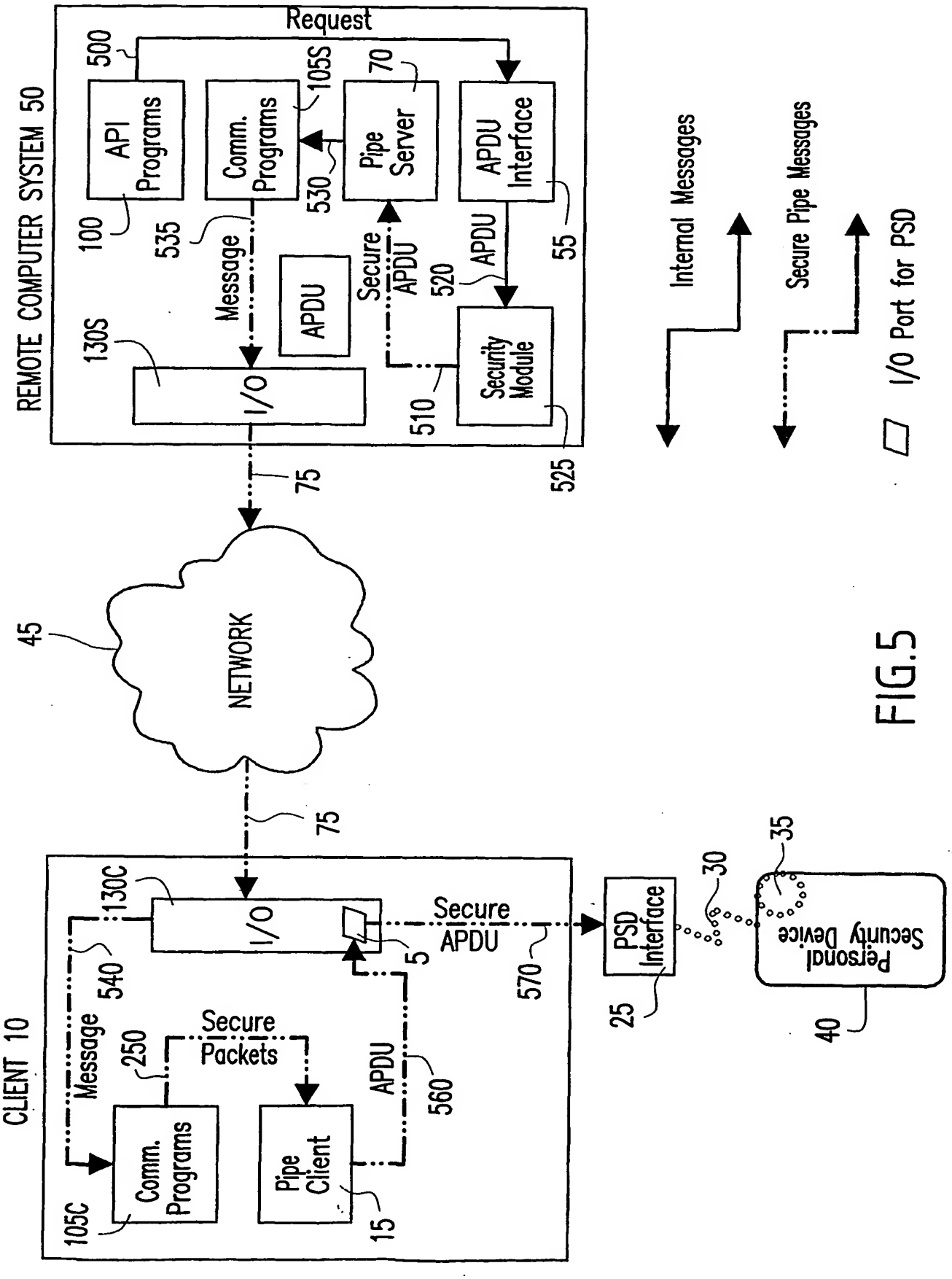

REMOTE COMPUTER SYSTEM 50
Request
500
API Programs
100
105S
Comm. Programs
535
70
Pipe Server
530
APDU Interface
55
Message
APDU
Secure APDU
520
APDU
130S
I/O
510
Security Module
525
75
NETWORK
45
75
CLIENT 10
130C
I/O
Secure APDU
5
570
540
Message
250
Secure Packets
APDU
560
105C
Comm. Programs
Pipe Client
15
PSD Interface
25
30
35
Personal Security Device
40
Internal Messages
Secure Pipe Messages
I/O Port for PSD

FIG.5

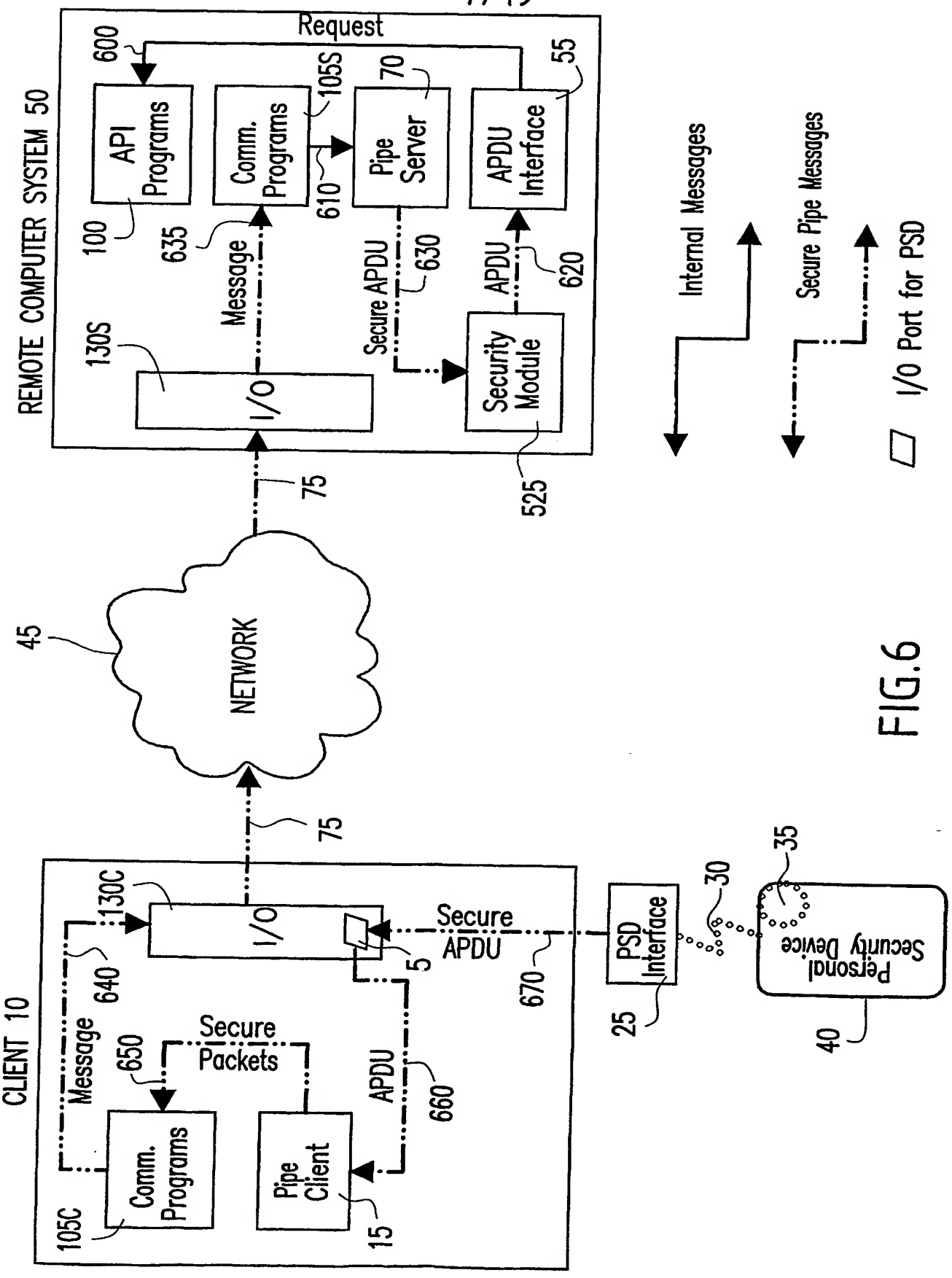
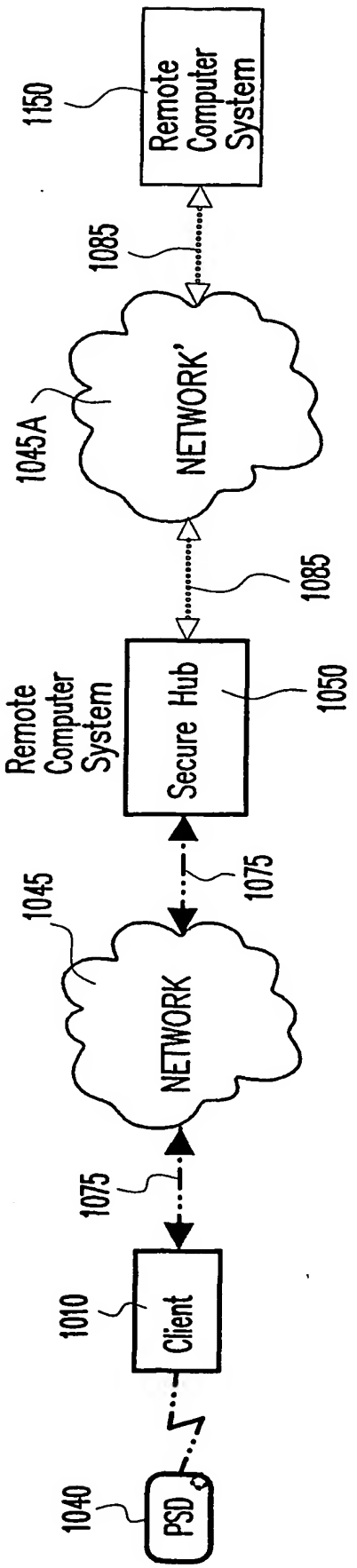

REMOTE COMPUTER SYSTEM 50
Request
600
API Programs
100
Comm. Programs
105S
635
Message
610
Pipe Server
Secure APDU
630
APDU Interface
55
APDU
620
130S
I/O
Security Module
525
75
NETWORK
45
75
CLIENT 10
130C
I/O
Secure APDU
5
640
Message
650
Secure Packets
APDU
660
Comm. Programs
105C
Pipe Client
15
670
PSD Interface
25
30
35
Personal Security Device
40
Internal Messages
Secure Pipe Messages
I/O Port for PSD

FIG.6


1150
Remote Computer System
1085
1045A
NETWORK'
1085
Remote Computer System
Secure Hub
1050
1075
1045
NETWORK
1075
1010
Client
1040
PSD

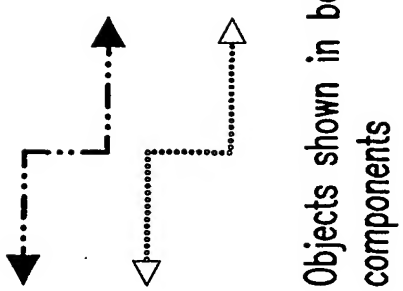

Secure Pipe Messages
Remote Messaging
Objects shown in bold indicate secure active components

FIG.7

FIG.8

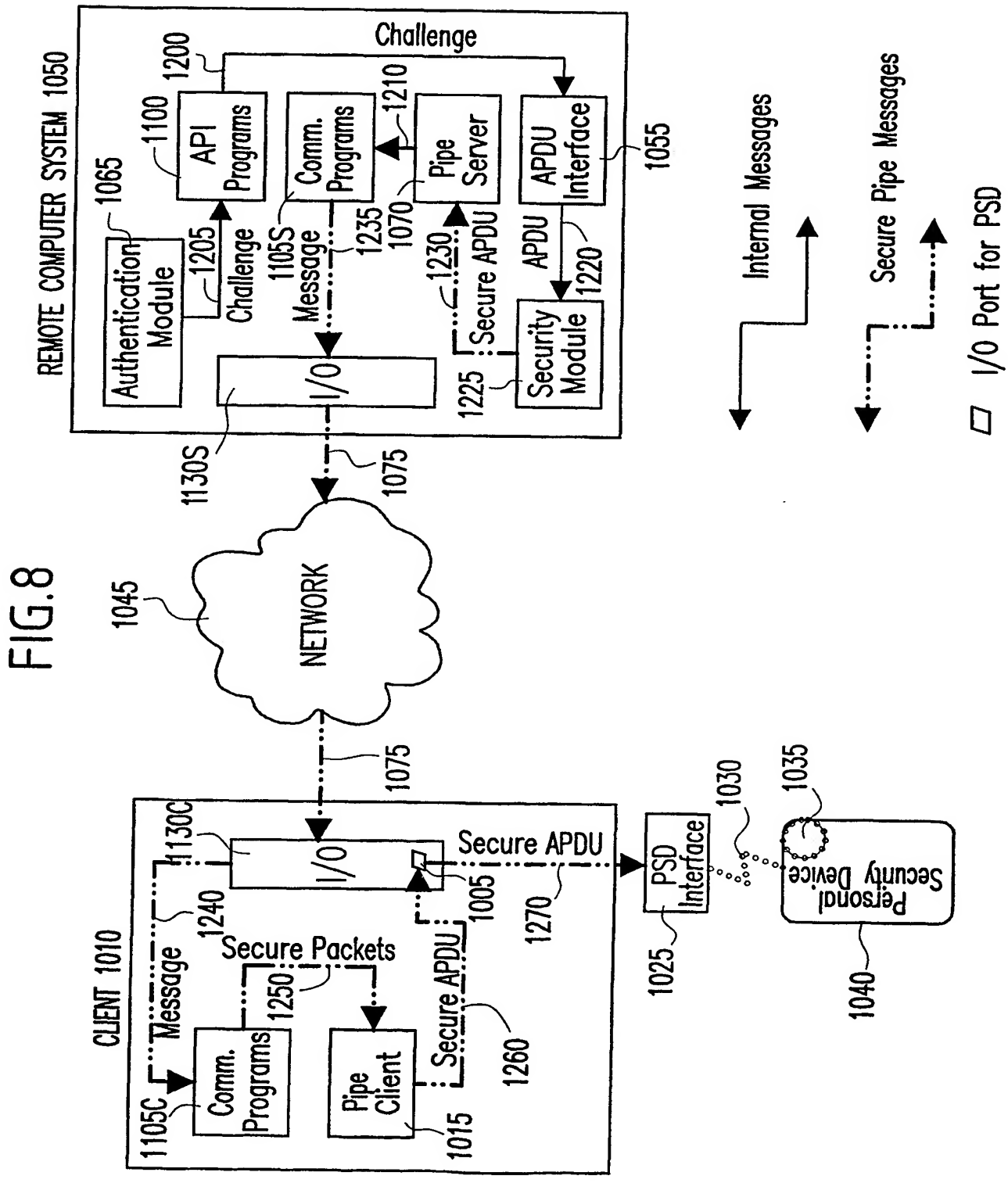

REMOTE COMPUTER SYSTEM 1050
Challenge
1200
1100
API Programs
1210
Comm. Programs
Pipe Server
APDU Interface
1055
1065
Authentication Module
1205
Challenge
1105S
Message
1235
1070
1230
Secure APDU
APDU
1220
1225
Security Module
I/O
1130S
1075
NETWORK
1045
Internal Messages
Secure Pipe Messages
I/O Port for PSD
CLIENT 1010
1130C
I/O
Secure APDU
1005
1270
1240
Message
Secure Packets
1250
Secure APDU
1260
1105C
Comm. Programs
Pipe Client
1015
PSD Interface
1025
1030
1035
Personal Security Device
1040

FIG.9

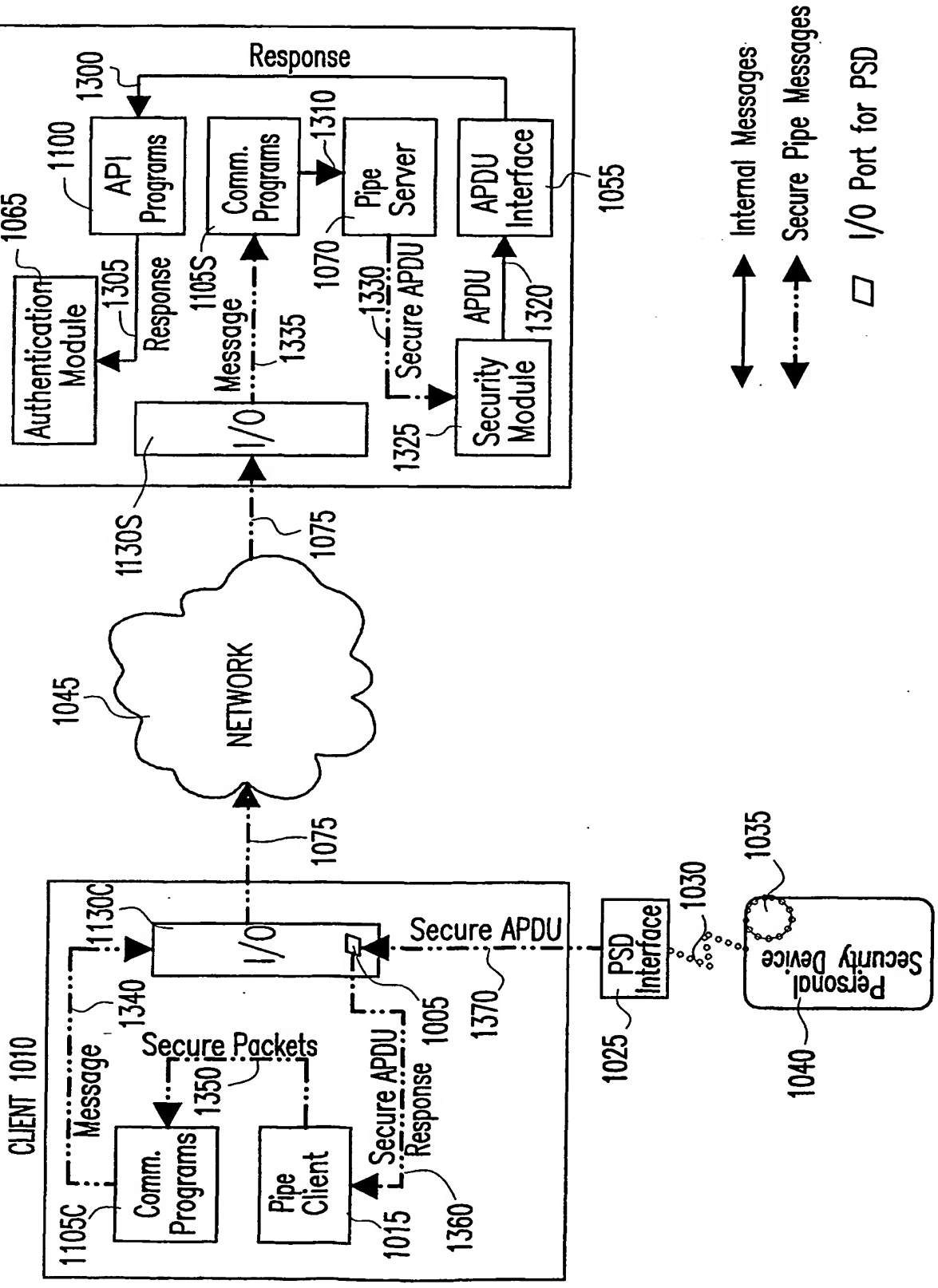

Response
1300
1100
API Programs
Comm. Programs
1310
Pipe Server
APDU Interface
1055
1065
Authentication Module
1305
Response
1105S
Message
1335
1070
1330
Secure APDU
APDU
1320
1130S
I/O
1325
Security Module
1075
1045
NETWORK
1075
1130C
I/O
Secure APDU
1340
1005
1370
Secure Packets
1350
Message
CLIENT 1010
1105C
Comm. Programs
Pipe Client
Secure APDU
Response
1015
1360
PSD Interface
1025
1030
1035
Personal Security Device
1040
Internal Messages
Secure Pipe Messages
I/O Port for PSD

FIG.10

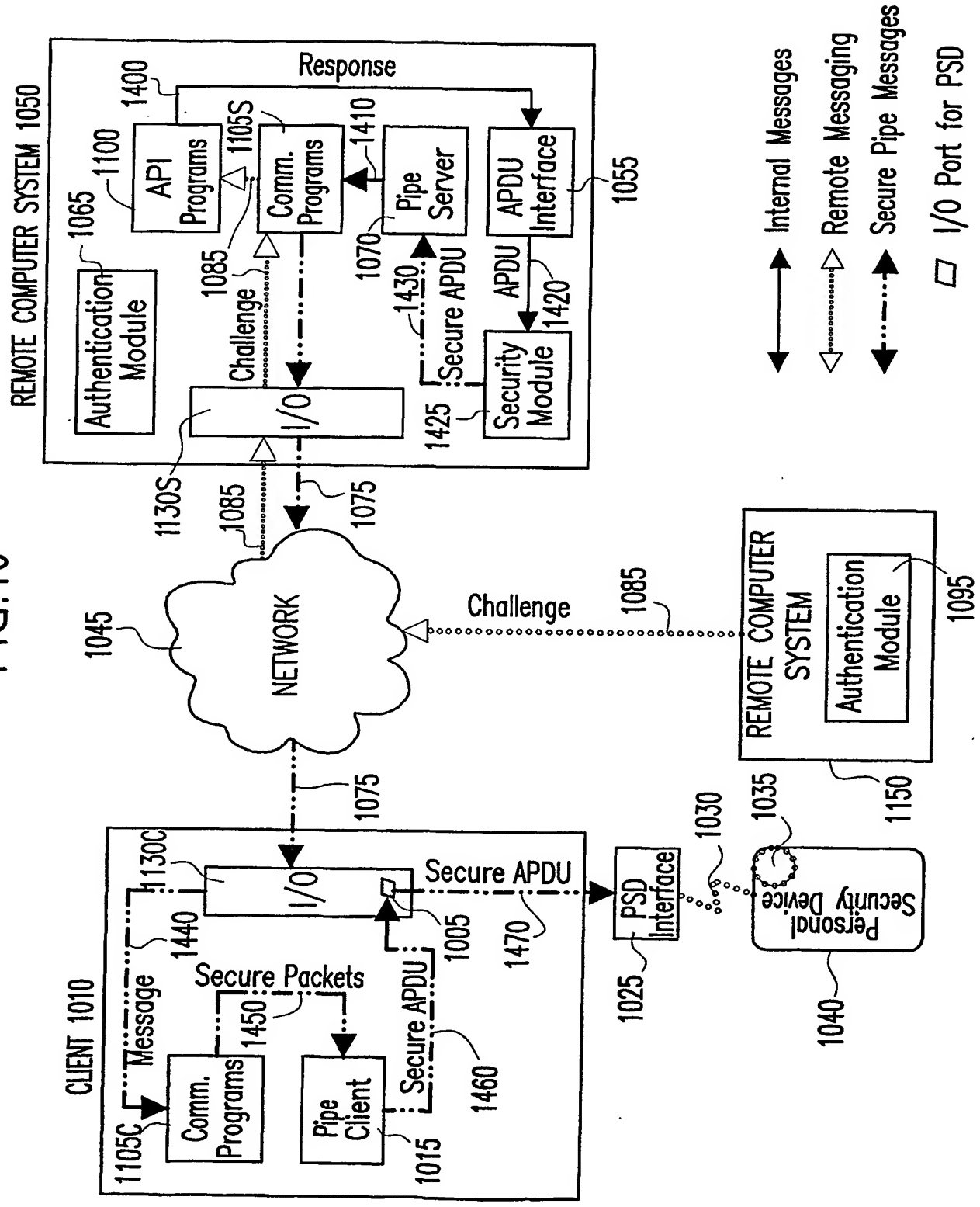

REMOTE COMPUTER SYSTEM 1050
Response
1400
API Programs
1100
1105S
Comm. Programs
1410
Pipe Server
APDU Interface
1055
1065
Authentication Module
1085
Challenge
1070
1430
Secure APDU
APDU
1420
Security Module
1425
I/O
1130S
1085
1075
NETWORK
1045
Challenge
1085
REMOTE COMPUTER SYSTEM
Authentication Module
1095
1150
1075
CLIENT 1010
1130C
I/O
Secure APDU
1440
1005
1470
Message
Secure Packets
1450
Secure APDU
1460
1105C
Comm. Programs
Pipe Client
1015
PSD Interface
1025
1030
1035
Personal Security Device
1040
Internal Messages
Remote Messaging
Secure Pipe Messages
I/O Port for PSD

FIG.11

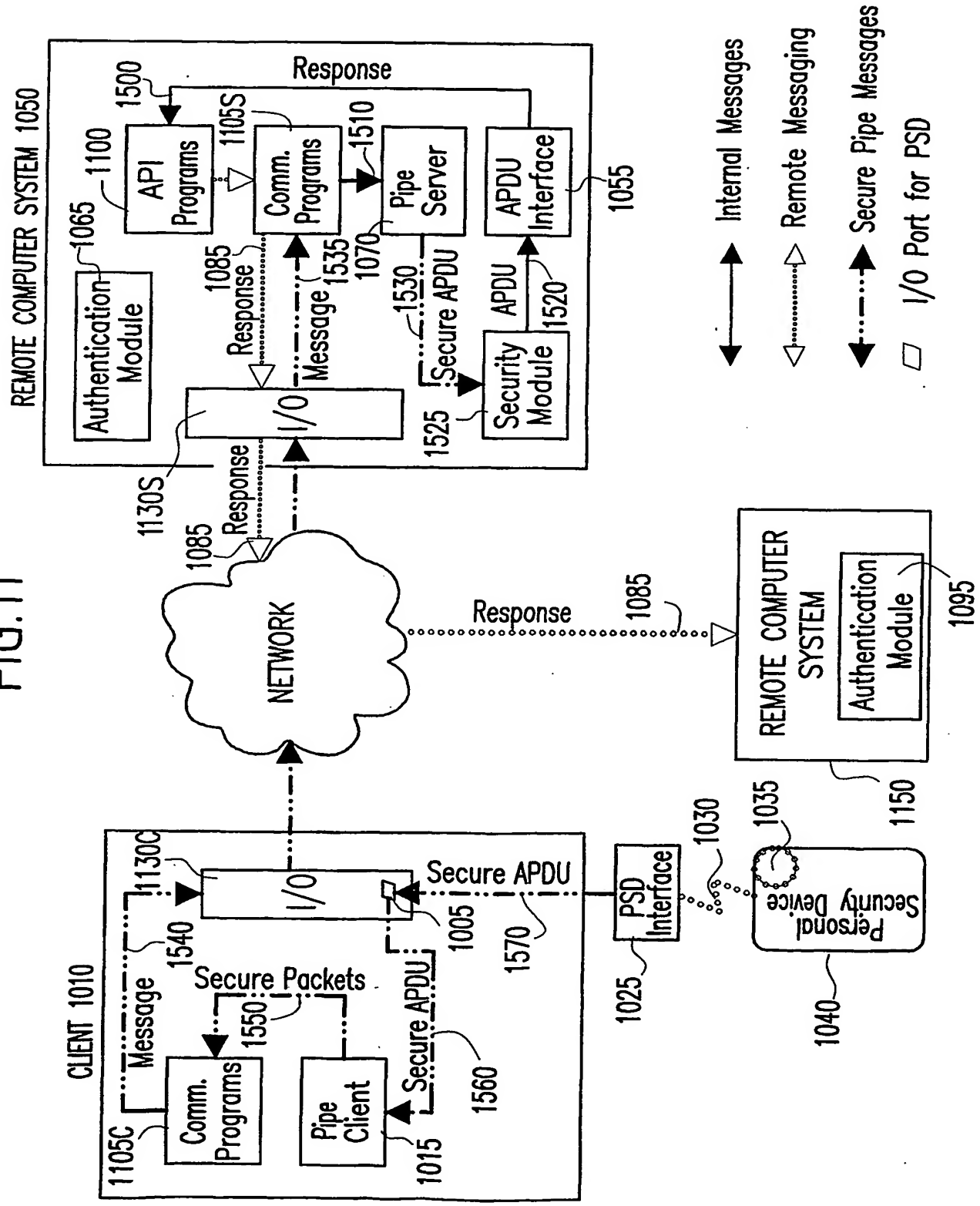

REMOTE COMPUTER SYSTEM 1050
Response
1500
API Programs
1100
1105S
Comm. Programs
1510
Pipe Server
APDU Interface
1055
1065
Authentication Module
1085
Response
1535
Message
1070
1530
Secure APDU
APDU
1520
Security Module
1525
I/O
1130S
Response
1085
NETWORK
Response
1085
REMOTE COMPUTER SYSTEM
Authentication Module
1095
1150
CLIENT 1010
1130C
I/O
Secure APDU
1005
1570
1540
Message
Secure Packets
1550
Secure APDU
1560
1105C
Comm. Programs
Pipe Client
1015
PSD Interface
1025
1030
1035
Personal Security Device
1040
Internal Messages
Remote Messaging
Secure Pipe Messages
I/O Port for PSD

FIG.12

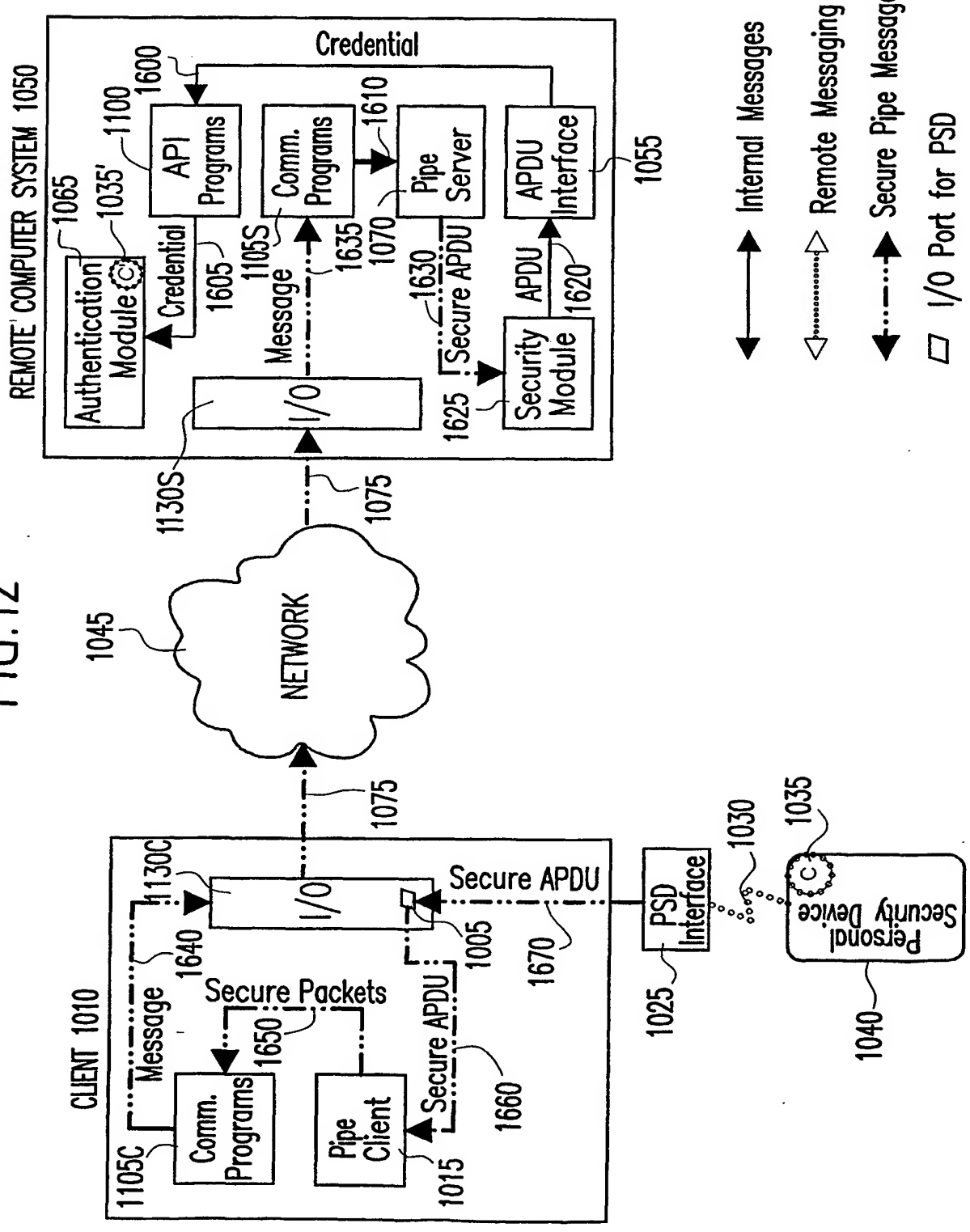

REMOTE COMPUTER SYSTEM 1050
Credential
1600
API Programs
1100
Comm. Programs
1610
Pipe Server
APDU Interface
1055
1065
1035'
Authentication Module
Credential
1605
1105S
Message
1635
1070
1630
Secure APDU
APDU
1620
1625
Security Module
I/O
1130S
1075
NETWORK
1045
1075
CLIENT 1010
1130C
I/O
Secure APDU
1640
1005
1670
Message
Secure Packets
1650
1105C
Comm. Programs
Pipe Client
Secure APDU
1660
1015
PSD Interface
1025
1030
1035
Personal Security Device
1040
Internal Messages
Remote Messaging
Secure Pipe Messages
I/O Port for PSD

FIG.13

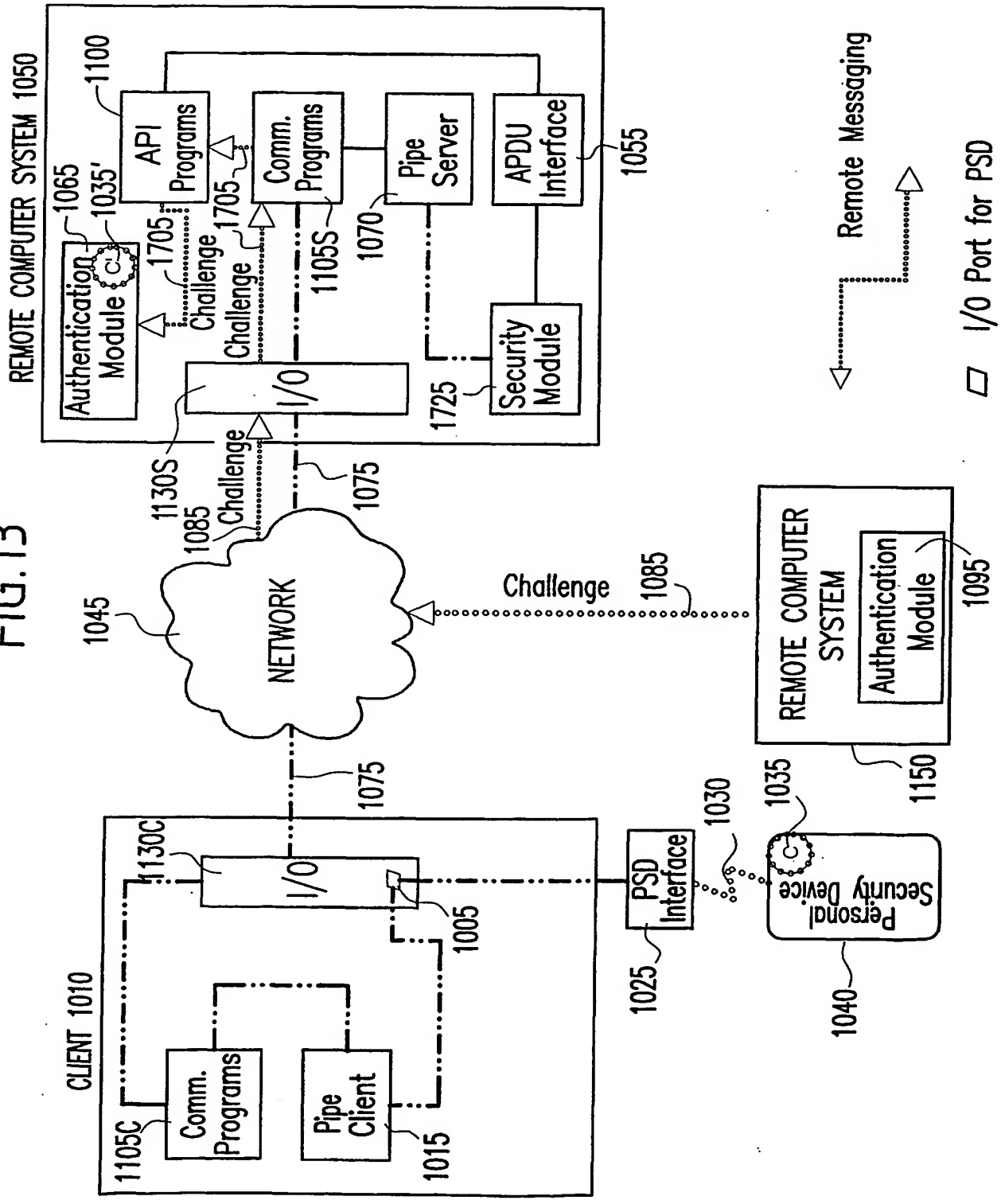

REMOTE COMPUTER SYSTEM 1050
1100
API Programs
Comm. Programs
Pipe Server
APDU Interface
1055
1065
1035'
Authentication Module
1705
Challenge
1705
Challenge
1105S
1070
1725
Security Module
I/O
1130S
Challenge
1085
1075
NETWORK
1045
Challenge
1085
REMOTE COMPUTER SYSTEM
Authentication Module
1095
1150
1075
1130C
I/O
1005
PSD Interface
1030
1035
Personal Security Device
1040
1025
CLIENT 1010
1105C
Comm. Programs
Pipe Client
1015
Remote Messaging
I/O Port for PSD

FIG.14

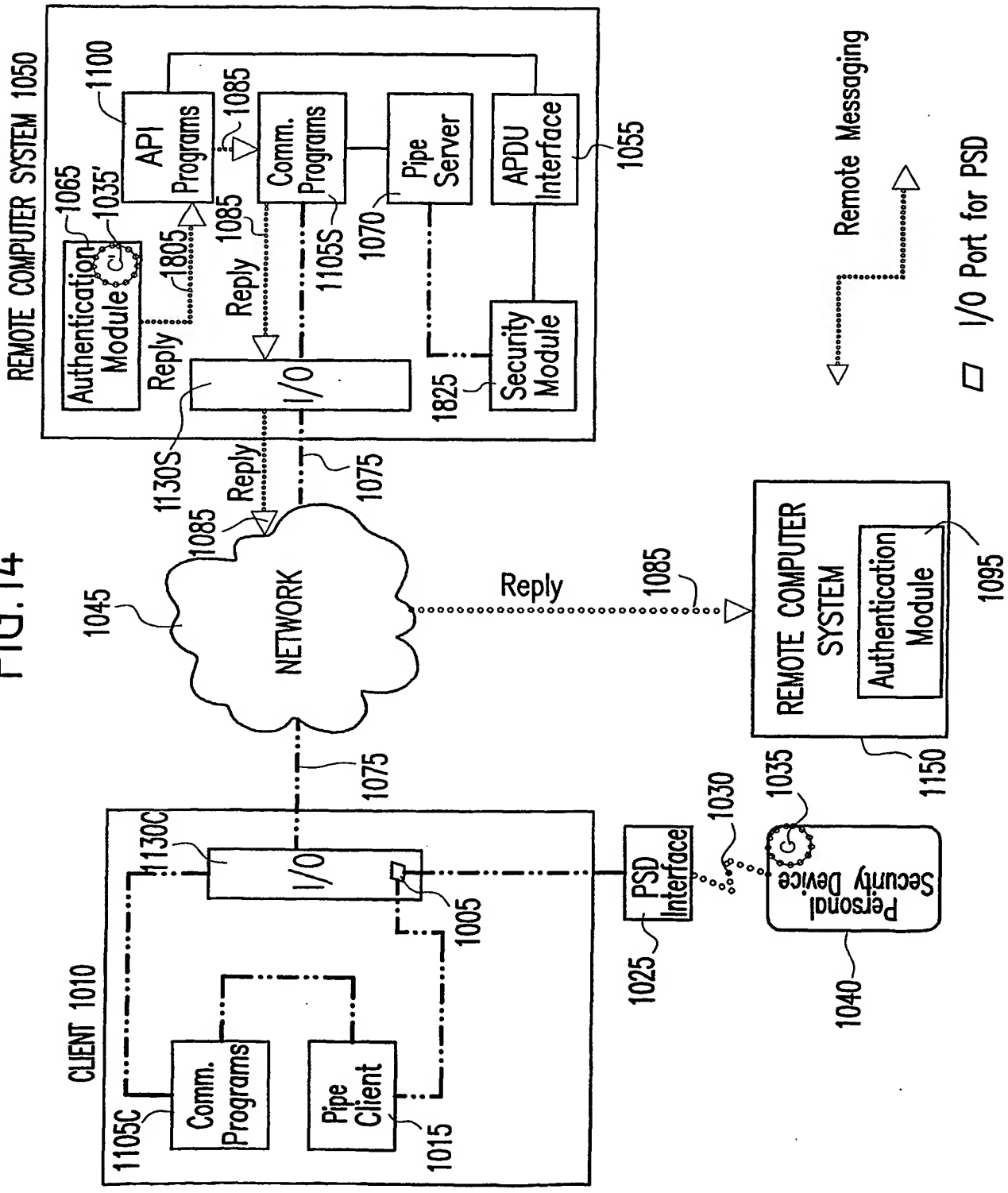

REMOTE COMPUTER SYSTEM 1050
1100
API Programs
1085
Comm. Programs
Pipe Server
APDU Interface
1055
1065
1035'
Authentication Module
1805
Reply
1085
Reply
1105S
1070
1130S
Reply
1085
1075
I/O
1825
Security Module
Remote Messaging
I/O Port for PSD
1045
NETWORK
Reply
1085
REMOTE COMPUTER SYSTEM
Authentication Module
1095
1150
1075
1130C
I/O
1005
PSD Interface
1030
1035
Personal Security Device
1040
1025
CLIENT 1010
1105C
Comm. Programs
Pipe Client
1015

FIG.15A

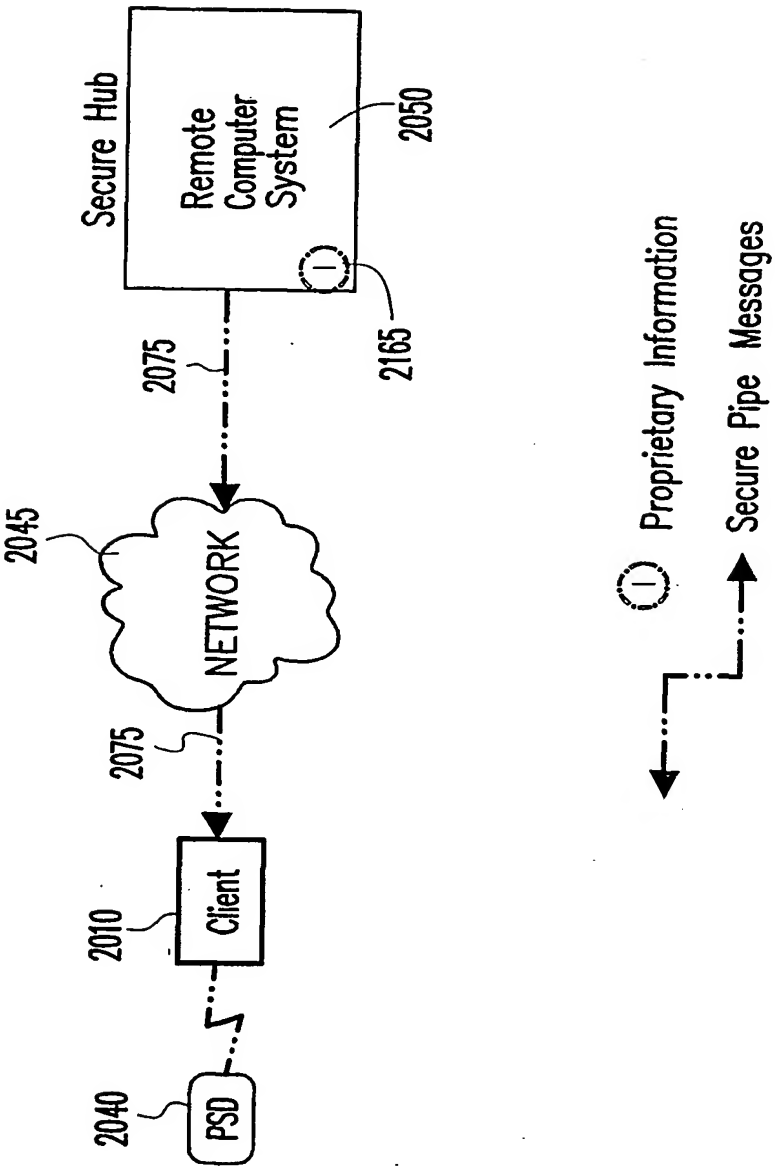
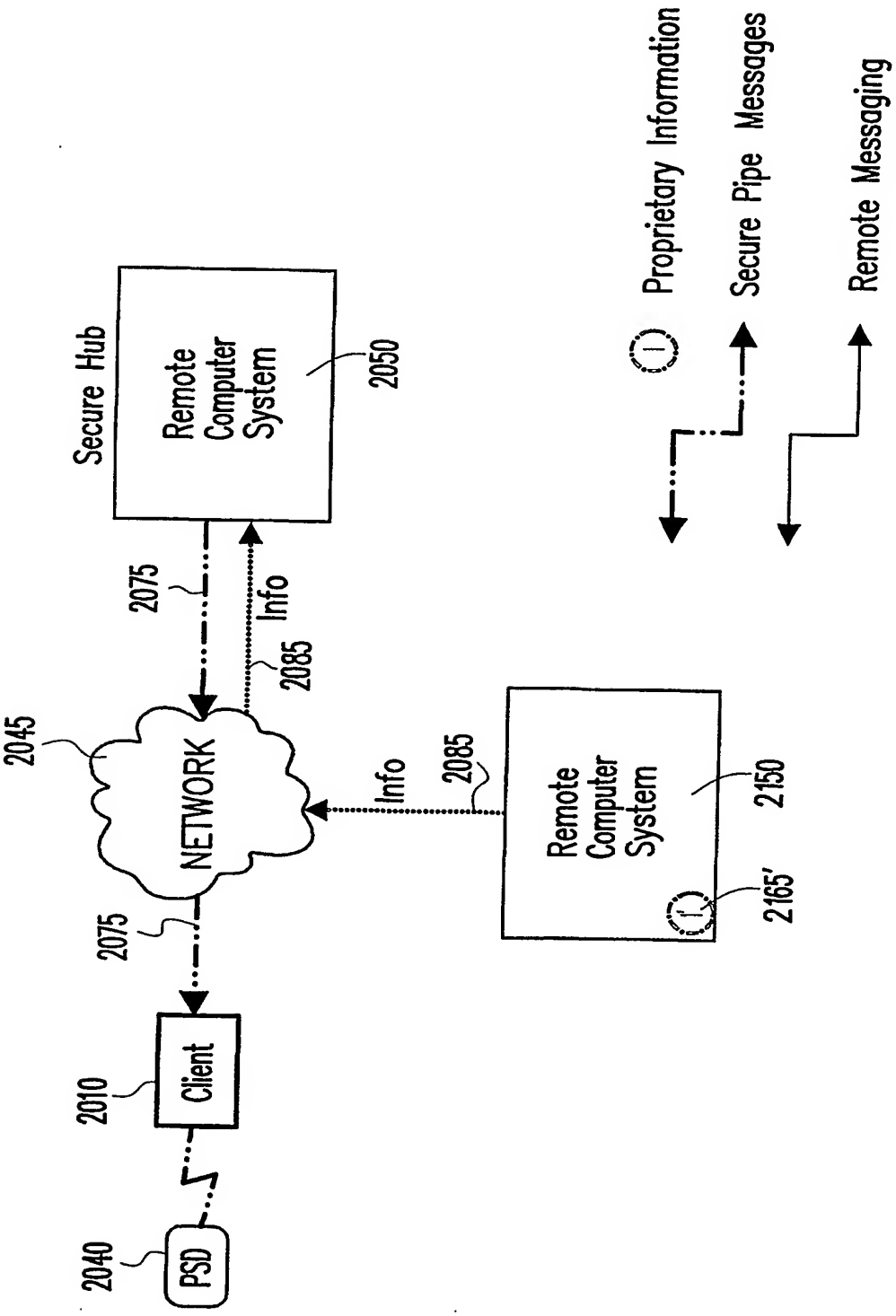

Secure Hub
Remote Computer System
2050
2165
2075
2045
NETWORK
2075
2010
Client
2040
PSD
Proprietary Information
Secure Pipe Messages

FIG.15B


Secure Hub
Remote Computer System
2050
2075
Info
2085
2045
NETWORK
Info
2085
Remote Computer System
2150
2165'
2075
2010
Client
2040
PSD
Proprietary Information
Secure Pipe Messages
Remote Messaging

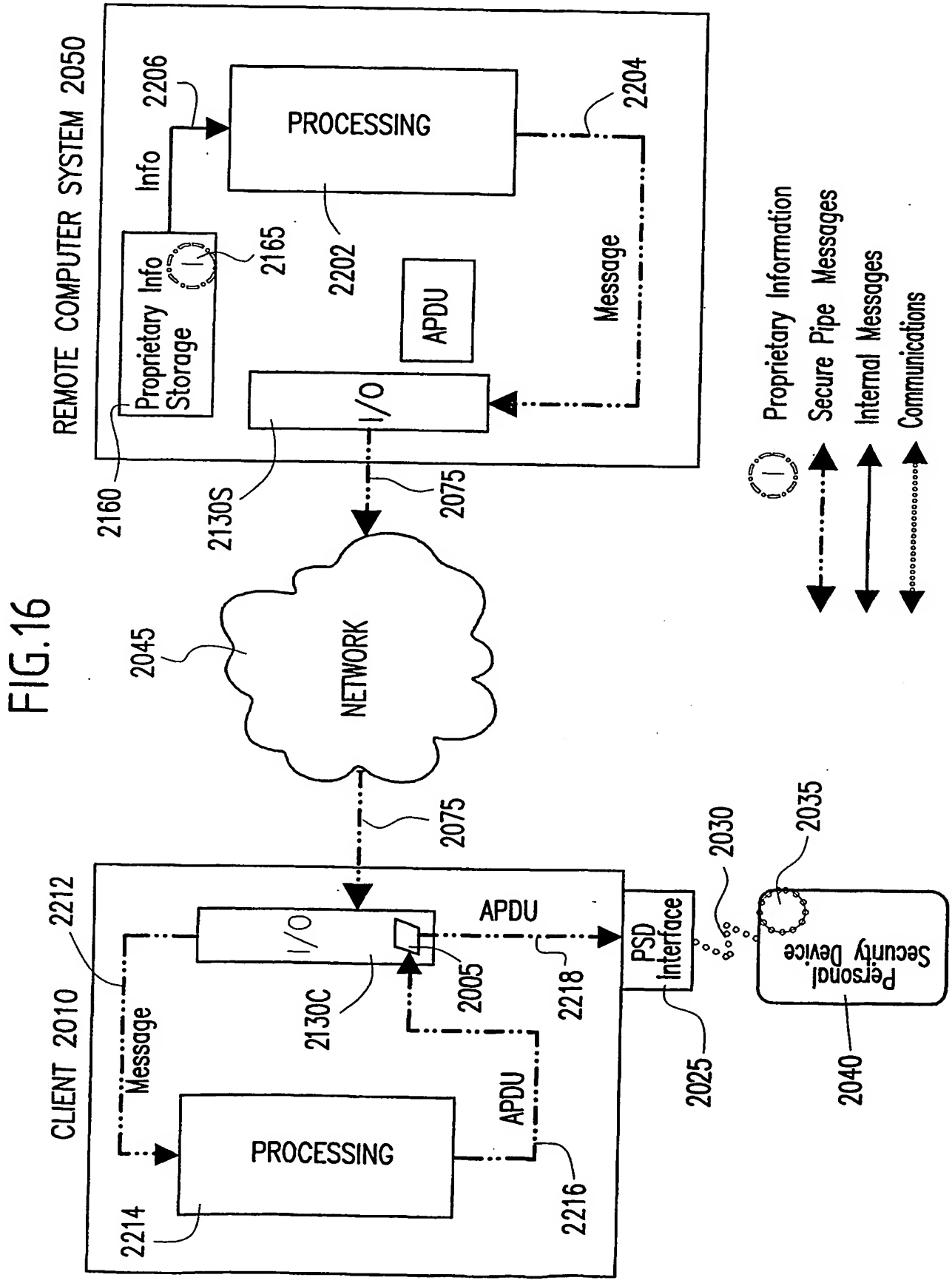
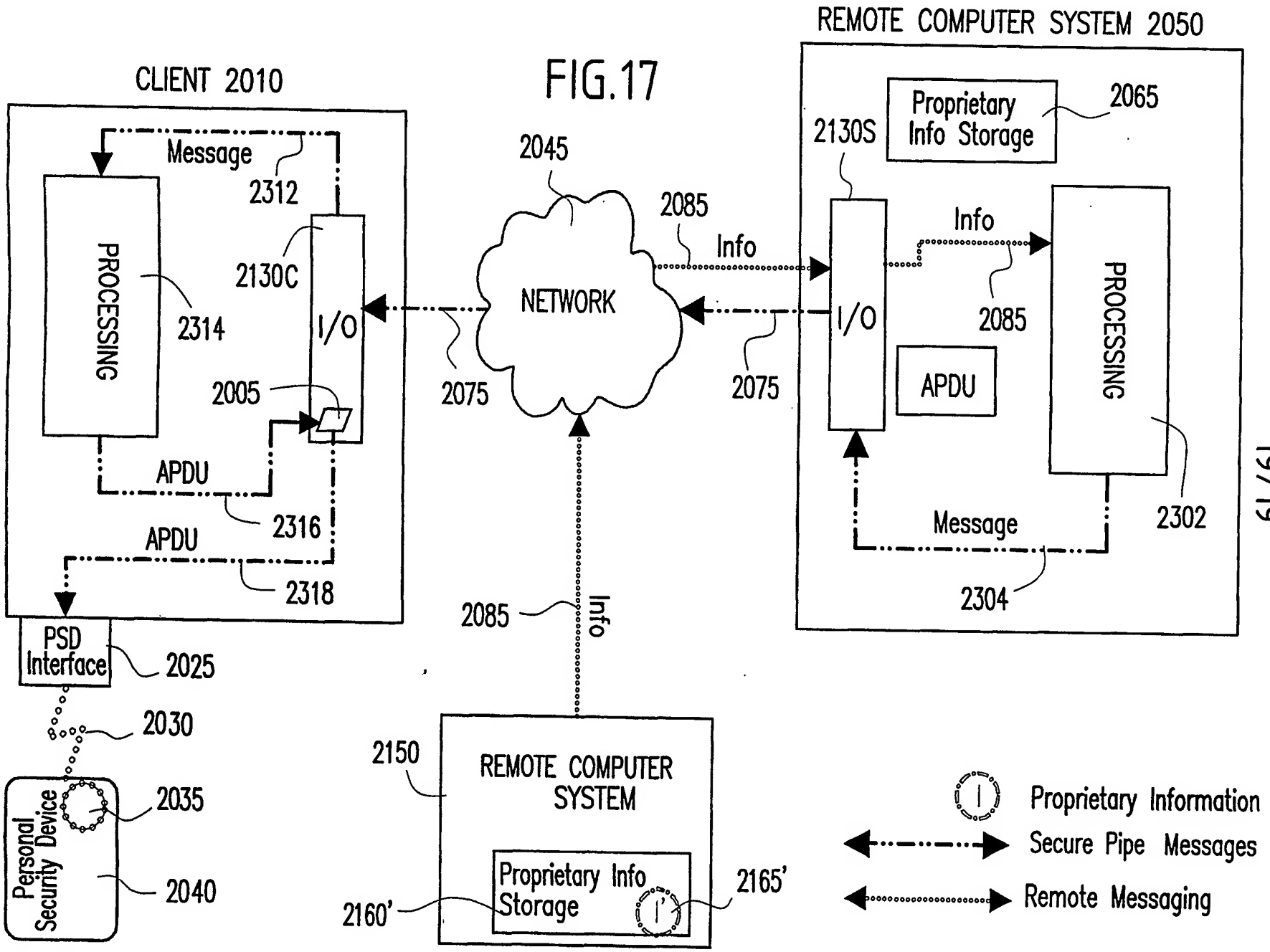

REMOTE COMPUTER SYSTEM 2050
PROCESSING
2206
Info
2204
2202
2165
Proprietary Info Storage
APDU
Message
I/O
2160
2130S
2075
Proprietary Information
Secure Pipe Messages
Internal Messages
Communications
NETWORK
2045
2075
CLIENT 2010
2212
Message
I/O
APDU
2130C
2005
2218
PSD Interface
2030
2035
Personal Security Device
2025
2040
PROCESSING
APDU
2214
2216

FIG.16

FIG.17


CLIENT 2010
Message
2312
PROCESSING
2314
2130C
I/O
2005
APDU
2316
APDU
2318
PSD Interface
2025
2030
Personal Security Device
2035
2040
2045
NETWORK
2085
Info
2075
2085
Info
2075
REMOTE COMPUTER SYSTEM 2050
2130S
Proprietary Info Storage
2065
I/O
Info
2085
PROCESSING
APDU
Message
2302
2304
2150
REMOTE COMPUTER SYSTEM
Proprietary Info Storage
2160'
2165'
Proprietary Information
Secure Pipe Messages
Remote Messaging

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 02/03930

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 52161 A (MONDEX INT LTD) 19 November 1998 (1998-11-19) page 3, line 14 -page 4, line 3 page 4, line 16 -page 5, line 4 page 48, line 18 - line 23 figure 1 claim 18 ---	1-15
P,X	WO 01 59730 A (KEYCORP LTD ;GHYS STANLEY (AU)) 16 August 2001 (2001-08-16) abstract page 1, line 11 -page 3, line 24 figure 3A ---	1-15
A	EP 0 911 772 A (CITICORP DEV CENTER INC) 28 April 1999 (1999-04-28) the whole document ---	1-15

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 August 2002	23/08/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bub, A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 02/03930

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 195 22 527 A (IBM) 2 January 1997 (1997-01-02) page 5, line 24 - line 38 claims 10,31 figure 3	4,5, 13-15

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 02/03930

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9852161	A	19-11-1998	US	6385723 B1	07-05-2002
			AU	736325 B2	26-07-2001
			AU	6299698 A	09-09-1998
			AU	7776798 A	08-12-1998
			AU	7776898 A	08-12-1998
			AU	7776998 A	08-12-1998
			AU	7777098 A	08-12-1998
			AU	7777198 A	08-12-1998
			AU	7777298 A	08-12-1998
			AU	7777398 A	08-12-1998
			AU	7777498 A	08-12-1998
			EP	0963580 A1	15-12-1999
			EP	0981807 A2	01-03-2000
			EP	0985202 A1	15-03-2000
			EP	0985203 A1	15-03-2000
			EP	0976114 A2	02-02-2000
			EP	0985204 A1	15-03-2000
			EP	0981805 A1	01-03-2000
			WO	9837526 A1	27-08-1998
			WO	9852158 A2	19-11-1998
			WO	9852159 A2	19-11-1998
			WO	9852160 A2	19-11-1998
			WO	9852161 A2	19-11-1998
			WO	9852152 A2	19-11-1998
			WO	9852162 A2	19-11-1998
			WO	9852163 A2	19-11-1998
			WO	9852153 A2	19-11-1998
			JP	2001513231 T	28-08-2001
			JP	2001525956 T	11-12-2001
			JP	2001527674 T	25-12-2001
			JP	2001525957 T	11-12-2001
			JP	2002512715 T	23-04-2002
			JP	2001527675 T	25-12-2001
			JP	2001525958 T	11-12-2001
			US	2002050528 A1	02-05-2002
			US	6220510 B1	24-04-2001
			US	6230267 B1	08-05-2001
			US	6164549 A	26-12-2000
			US	6317832 B1	13-11-2001
			US	6328217 B1	11-12-2001
			US	2001056536 A1	27-12-2001
WO 0159730	A	16-08-2001	WO	0159730 A1	16-08-2001
			AU	3142001 A	20-08-2001
EP 0911772	A	28-04-1999	EP	0911772 A2	28-04-1999
			US	6422459 B1	23-07-2002
DE 19522527	A	02-01-1997	DE	19522527 A1	02-01-1997
			WO	9701147 A2	09-01-1997
			HU	9800977 A2	28-08-1998
			JP	9510812 T	28-10-1997
			PL	318655 A1	07-07-1997
			US	6279047 B1	21-08-2001